THE DISTRIBUTION OF TOTIENTS

KEVIN FORD

Dedicated to the memory of Paul Erdős (1913–1996)

ABSTRACT. This paper is a comprehensive study of the set of totients, i.e. the set of values taken by Euler's ϕ-function. We fist determine the true order of magnitude of $V(x)$, the number of totients $\leqslant x$. We also show that if there is a totient with exactly k preimages under ϕ (a totient with "multiplicity" k), then the counting function for such totients, $V_k(x)$, satisfies $V_k(x) \gg_k V(x)$. Sierpiński conjectured that every multiplicity $k \geqslant 2$ is possible, and we deduce this from the Prime k-tuples Conjecture. We also make some progress toward an older conjecture of Carmichael, which states that no totient has multiplicity 1. The lower bound for a possible counterexample is extended to $10^{10^{10}}$ and the bound $\liminf_{x\to\infty} V_1(x)/V(x) \leqslant 10^{-5,000,000,000}$ is shown. Determining the order of $V(x)$ and $V_k(x)$ also provides a description of the "normal" multiplicative structure of totients. This takes the form of bounds on the sizes of the prime factors of a pre-image of a typical totient. One corollary is that the normal number of prime factors of a totient $\leqslant x$ is $c \log\log x$, where $c \approx 2.186$. Similar results are proved for the set of values taken by a general multiplicative arithmetic function, such as the sum of divisors function, whose behavior is similar to that of Euler's function.

1 Introduction

Let $\mathscr{V}$ denote the set of values taken by Euler's ϕ-function (totients), i.e.

$$\mathscr{V} = \{1, 2, 4, 6, 8, 10, 12, 16, 18, 20, 22, 24, 28, 30, \cdots\}.$$

Let

$$\begin{aligned} \mathscr{V}(x) &= \mathscr{V} \cap [1, x], \\ V(x) &= |\mathscr{V}(x)|, \\ \phi^{-1}(m) &= \{n : \phi(n) = m\}, \\ A(m) &= |\phi^{-1}(m)|, \\ V_k(x) &= |\{m \leqslant x : A(m) = k\}|. \end{aligned} \tag{1.1}$$

We will refer to $A(m)$ as the multiplicity of m. This paper is concerned with the following problems.

1. What is the order of $V(x)$?
2. What is the order of $V_k(x)$ when the multiplicity k is possible?
3. What multiplicities are possible?
4. What is the normal multiplicative structure of totients?

1991 *Mathematics Subject Classification.* Primary 11A25, 11N64.

Keywords: Euler's function, totients, Carmichael's Conjecture, Sierpiński's Conjecture.

Much of the early work for this paper was completed while the author was enjoying the hospitality of the Institute for Advanced Study, supported by National Science Foundation grant DMS 9304580.

1.1 The order of $V(x)$

The fact that $\phi(p) = p - 1$ for primes p implies $V(x) \gg x/\log x$ by the Prime Number Theorem. Pillai [28] gave the first non-trivial upper bound on $V(x)$, namely

$$V(x) \ll \frac{x}{(\log x)^{(\log 2)/e}}.$$

Using sieve methods, Erdős [8] improved this to

$$V(x) \ll_\varepsilon \frac{x}{(\log x)^{1-\varepsilon}}$$

for every $\varepsilon > 0$. Upper and lower bounds for $V(x)$ were sharpened in a series of papers by Erdős [9], Erdős and Hall [11, 12], Pomerance [29], and finally by Maier and Pomerance [26], who showed that

$$V(x) = \frac{x}{\log x} \exp\{(C + o(1))(\log_3 x)^2\} \tag{1.2}$$

for a constant C defined below. Here $\log_k x$ denotes the kth iterate of the logarithm. Let

$$F(x) = \sum_{n=1}^{\infty} a_n x^n, \qquad a_n = (n+1)\log(n+1) - n\log n - 1. \tag{1.3}$$

Since $a_n \sim \log n$ and $a_n > 0$, it follows that $F(x)$ is defined and strictly increasing on $[0, 1)$, $F(0) = 0$ and $F(x) \to \infty$ as $x \to 1^-$. Thus, there is a unique number ϱ such that

$$F(\varrho) = 1 \qquad (\varrho = 0.542598586098471021959\ldots). \tag{1.4}$$

In addition, $F'(x)$ is strictly increasing, and

$$F'(\varrho) = 5.69775893423019267575\ldots$$

Let

$$C = \frac{1}{2|\log \varrho|} = 0.81781464640083632231\ldots \tag{1.5}$$

and

$$\begin{aligned} D &= 2C(1 + \log F'(\varrho) - \log(2C)) - 3/2 \\ &= 2.17696874355941032173\ldots \end{aligned} \tag{1.6}$$

Our main result is a determination of the true order of $V(x)$.

Theorem 1. *We have*

$$V(x) = \frac{x}{\log x} \exp\{C(\log_3 x - \log_4 x)^2 + D\log_3 x - (D + 1/2 - 2C)\log_4 x + O(1)\}.$$

1.2 The order of $V_k(x)$

Erdős [10] showed by sieve methods that if $A(m) = k$, then for most primes p, $A(m(p-1)) = k$. If the multiplicity k is possible, then $V_k(x) \gg x/\log x$. Applying the machinery used to prove Theorem 1, we show that if there exists m with $A(m) = k$, then a positive proportion of totients have multiplicity k.

Theorem 2. *For every $\varepsilon > 0$, if $A(d) = k$, then*

$$V_k(x) \gg_\varepsilon d^{-1-\varepsilon} V(x) \qquad (x \geqslant x_0(d)).$$

Conjecture 1. *For $k \geqslant 2$,*

$$\lim_{x\to\infty} \frac{V_k(x)}{V(x)} = C_k.$$

x	$V(x)$	V_2/V	V_3/V	V_4/V	V_5/V	V_6/V	V_7/V
1M	180,184	0.380727	0.140673	0.098988	0.042545	0.062730	0.020790
5M	840,178	0.379462	0.140350	0.102487	0.042687	0.063193	0.020373
10M	1,634,372	0.378719	0.140399	0.103927	0.042703	0.063216	0.020061
25M	3,946,809	0.378198	0.140233	0.105466	0.042602	0.063414	0.019819
125M	18,657,531	0.377218	0.140176	0.107873	0.042560	0.063742	0.019454
300M	43,525,579	0.376828	0.140170	0.108933	0.042517	0.063818	0.019284
500M	71,399,658	0.376690	0.140125	0.109509	0.042493	0.063851	0.019194

TABLE 1. $V_k(x)/V(x)$ for $2 \leqslant k \leqslant 7$

Table 1 lists values of $V(x)$ and the ratios $V_k(x)/V(x)$ for $2 \leqslant k \leqslant 7$. Numerical investigations seem to indicate that $C_k \asymp 1/k^2$. In fact, at $x = 500,000,000$ we have $1.75 \leqslant V_k(x)/V(x) \leqslant 2.05$ for $20 \leqslant k \leqslant 200$. This data is very misleading, however. Erdős [8] showed that there are infinitely many totients for which $A(m) \geqslant m^{c_4}$ for some positive constant c_4. The current record is $c_4 = 0.7039$ [1]. Consequently, by Theorem 2, for infinitely many k we have

$$\frac{V_k(x)}{V(x)} \gg k^{-1/c_4+\varepsilon} \gg k^{-1.42} \qquad (x > x_0(k)).$$

Erdős has conjectured that every $c_4 < 1$ is admissible.

We also show that most totients have "essentially bounded" multiplicity.

Theorem 3. *Uniformly for $x \geqslant 2$ and $N \geqslant 2$, we have*

$$\frac{|\{m \in \mathscr{V}(x) : A(m) \geqslant N\}|}{V(x)} = \sum_{k \geqslant N} \frac{V_k(x)}{V(x)} \ll \exp\{-\tfrac{1}{4}(\log_2 N)^2\}.$$

Remark. The proof of [14, Theorem 3] contains an error, and the corrected proof (in Sec. 7.1 below) gives the weaker estimate given in Theorem 3.

In contrast, the average value of $A(m)$ over totients $m \leqslant x$ is clearly $\geqslant x/V(x) = (\log x)^{1+o(1)}$. The vast differences between the "average" behavior and the "normal" behavior is a result of some totients having enormous multiplicity.

A simple modification of the proof of Theorems 1 and 2 also gives bounds for totients in short intervals. A real number θ is said to be admissible if $\pi(x + x^\theta) - \pi(x) \gg x^\theta / \log x$ with x sufficiently large. Here, $\pi(x)$ is the number of primes $\leqslant x$. The current record is due to Baker, Harman and Pintz [2], who showed that $\theta = 0.525$ is admissible.

Theorem 4. *If θ is admissible, $y \geqslant x^\theta$ and the multiplicity k is possible, then*

$$V_k(x+y) - V_k(x) \asymp V(x+y) - V(x) \asymp \frac{y}{x+y} V(x+y).$$

Consequently, for every fixed $c > 1$, $V(cx) - V(x) \asymp_c V(x)$.

Erdős has asked if $V(cx) \sim cV(x)$ for each fixed $c > 1$, which would follow from an asymptotic formula for $V(x)$. The method of proof of Theorem 1, however, falls short of answering Erdős' question.

It is natural to ask what the maximum totient gaps are, in other words what is the behavior of the function $M(x) = \max_{v_i \leqslant x}(v_i - v_{i-1})$ if $v_1, v_2, \cdots$ denotes the sequence of totients? Can it be shown, for example, that for x sufficiently large, that there is a totient between x and $x + x^{1/2}$?

1.3 The conjectures of Carmichael and Sierpiński

In 1907, Carmichael [4] announced that for every m, the equation $\phi(x) = m$ has either no solutions x or at least two solutions. In other words, no totient can have multiplicity 1. His proof of this assertion was flawed, however, and the existence of such numbers remains an open problem. In [5], Carmichael did show that no number $m < 10^{37}$ has multiplicity 1, and conjectured that no such m exists (this is now known as Carmichael's Conjecture). Klee [24] improved the lower bound for a counterexample to 10^{400}, Masai and Valette [27] improved it to $10^{10,000}$ and recently Schlafly and Wagon [34] showed that a counterexample must exceed $10^{10,000,000}$. An immediate corollary of Theorem 2 (take $d = 1, k = 2$ for the first part) is

Theorem 5. *We have*

$$\limsup_{x\to\infty} \frac{V_1(x)}{V(x)} < 1.$$

Furthermore, Carmichael's Conjecture is equivalent to the bound

$$\liminf_{x\to\infty} \frac{V_1(x)}{V(x)} = 0.$$

Although this is a long way from proving Carmichael's Conjecture, Theorem 5 show that the set of counterexamples cannot be a "thin" subset of $\mathscr{V}$. Either there are no counterexamples or a positive fraction of totients are counterexamples.

The basis for the computations of lower bounds for a possible counterexample is a lemma of Carmichael and Klee (Lemma 7.2 below), which allows one to show that if $A(m) = 1$ then x must be divisible by the squares of many primes. Extending the method outlined in [34], we push the lower bound for a counterexample to Carmichael's Conjecture further.

Theorem 6. *If $A(m) = 1$, then $m \geqslant 10^{10^{10}}$.*

As a corollary, a variation of an argument of Pomerance [30] gives the following.

Theorem 7. *We have*

$$\liminf_{x\to\infty} \frac{V_1(x)}{V(x)} \leqslant 10^{-5,000,000,000}.$$

The proof of these theorems motivates another classification of totients. Let $V(x; k)$ be the number of totients up to x, all of whose pre-images are divisible by k. A trivial corollary to the proof of Theorem 2 is

Theorem 8. *If d is a totient, all of whose pre-images are divisible by k, then*

$$V(x; k) \gg_\varepsilon d^{-1-\varepsilon} V(x).$$

Thus, for each k, either $V(x; k) = 0$ for all x or $V(x; k) \gg_k V(x)$.

In the 1950's, Sierpiński conjectured that all multiplicities $k \geqslant 2$ are possible (see [31] and [10]), and in 1961, Schinzel [32] deduced this conjecture from his well-known Hypothesis H. Schinzel's Hypothesis H [33], a generalization of Dickson's Prime k-tuples Conjecture [7], states that any set of polynomials $F_1(n), \dots, F_k(n)$, subject to certain restrictions, are simultaneously prime for infinitely many n. Using a much simpler, iterative argument, we show that Sierpiński's Conjecture follows from the Prime k-tuples Conjecture.

Theorem 9. *The Prime k-tuples Conjecture implies that for each $k \geqslant 2$, there is a number d with $A(d) = k$.*

Shortly after [14] was published, the author and S. Konyagin proved Sierpiński's conjecture unconditionally for even k [15]. The conjecture for odd k was subsequently proved by the author [16] using a variant of Lemma 7.1 below.

1.4 The normal multiplicative structure of totients

Establishing Theorems 1 and 2 requires a determination of what a "normal" totient looks like. This will initially take the form of a series of linear inequalities in the prime factors of a pre-image of a totient. An analysis of these inequalities reveals the normal sizes of the prime factors of a pre-image of a typical totient. To state our results, we first define

$$L_0 = L_0(x) = \lfloor 2C(\log_3 x - \log_4 x)\rfloor. \tag{1.7}$$

In a simplified form, we show that for all but $o(V(x))$ totients $m \leqslant x$, every pre-image n satisfies

$$\log_2 q_i(n) \sim \varrho^i(1-i/L_0)\log_2 x \qquad (0 \leqslant i \leqslant L_0), \tag{1.8}$$

where $q_i(n)$ denotes the $(i+1)$st largest prime factor of n. For brevity, we write $V(x;\mathscr{C})$ for the number of totients $m \leqslant x$ which have a pre-image n satisfying condition $\mathscr{C}$. Also, let

$$\beta_i = \varrho^i(1-i/L_0) \qquad (0 \leqslant i \leqslant L_0 - 1).$$

Theorem 10. *Suppose* $1 \leqslant i \leqslant L_0$. *(a) If* $0 < \varepsilon \leqslant \frac{i}{3L_0}$, *then*

$$V\left(x; \left|\frac{\log_2 q_i(n)}{\beta_i \log_2 x} - 1\right| \geqslant \varepsilon\right) \ll V(x)\exp\left\{-\frac{L_0(L_0-i)}{4i}\varepsilon^2 + \log\left(\frac{i}{\varepsilon L_0}\right)\right\}.$$

(b) If $\frac{i}{3L_0} \leqslant \varepsilon \leqslant \frac{1}{8}$, *then*

$$V\left(x; \left|\frac{\log_2 q_i(n)}{\beta_i \log_2 x} - 1\right| \geqslant \varepsilon\right) \ll V(x)\exp\left\{-\tfrac{1}{13}L_0\varepsilon\right\}.$$

Using Theorem 10, we obtain a result about simultaneous approximation of $q_1(n), q_2(n), \ldots$.

Theorem 11. *Suppose* $L_0 = L_0(x)$, $0 \leqslant g \leqslant \frac{1}{3}\sqrt{\frac{L_0}{\log L_0}}$ *and* $0 \leqslant h \leqslant \frac{1}{2}L_0$. *The number of totients* $m \leqslant x$ *with a pre-image* n *not satisfying*

$$\left|\frac{\log_2 q_i(n)}{\beta_i \log_2 x} - 1\right| \geqslant g\sqrt{\frac{i\log(L_0-i)}{L_0(L_0-i)}} \qquad (1 \leqslant i \leqslant L_0 - h) \tag{1.9}$$

is

$$\ll V(x)\left(e^{-h/96} + e^{-\frac{1}{2}g^2\log g} + e^{-\frac{1}{14}g\sqrt{\log L_0}}\right).$$

Notice that the intervals in (1.9) are not only disjoint, but the gaps between them are rather large. In particular, this "discreteness phenomenon" means that for any $\varepsilon > 0$ and most totients $m \leqslant x$, no pre-image n has any prime factors p in the intervals

$$1-\varepsilon \geqslant \frac{\log_2 p}{\log_2 x} \geqslant \varrho + \varepsilon, \quad \varrho - \varepsilon \geqslant \frac{\log_2 p}{\log_2 x} \geqslant \varrho^2 + \varepsilon, \text{ etc.}$$

This should be compared to the distribution of the prime factors of a normal integer $n \leqslant x$ (e.g. Theorem 12 of [20]; see also subsection 1.5 below).

For a preimage n of a typical totient, we expect each $q_i(n)$ to be "normal", that is, $\omega(q_i(n)-1) \approx \log_2 q_i(n)$, where $\omega(m)$ is the number of distinct prime factors of m. This suggests that for a typical totient $v \leqslant x$,

$$\Omega(v) \approx \omega(v) \approx (1 + \varrho + \varrho^2 + \cdots)\log_2 x = \frac{\log_2 x}{1-\varrho}.$$

Theorem 12. *Suppose* $\eta = \eta(x)$ *satisfies* $0 \leqslant \eta \leqslant 1/3$. *Then*

$$\#\left\{m \in \mathscr{V}(x) : \left|\frac{\Omega(m)}{\log_2 x} - \frac{1}{1-\varrho}\right| \geqslant \eta\right\} \ll \frac{V(x)}{(\log_2 x)^{\eta/10}}.$$

Consequently, if $g(x)\to\infty$ arbitrarily slowly, then almost all totients $m\leqslant x$ satisfy

$$\left|\frac{\Omega(m)}{\log_2 x}-\frac{1}{1-\varrho}\right|\leqslant\frac{g(x)}{\log_3 x}.$$

Moreover, the theorem holds with $\Omega(m)$ replaced by $\omega(m)$.

Corollary 13. *If either $g(m)=\omega(m)$ or $g(m)=\Omega(m)$, then*

$$\sum_{m\in\mathscr{V}(x)} g(m)=\frac{V(x)\log_2 x}{1-\varrho}\left(1+O\left(\frac{1}{\log_3 x}\right)\right).$$

By contrast, Erdős and Pomerance [13] showed that the average of $\Omega(\phi(n))$, where the average is taken over all $n\leqslant x$, is $\frac{1}{2}(\log_2 x)^2+O((\log_2 x)^{3/2})$.

1.5 Heuristic arguments

As the details of the proofs of these results are very complex, we summarize the central ideas here. For most integers m, the prime divisors of m are "nicely distributed", meaning the number of prime factors of m lying between a and b is about $\log_2 b-\log_2 a$. This is a more precise version of the classical result of Hardy and Ramanujan [22] that most numbers m have about $\log_2 m$ prime factors. Take an integer n with prime factorization $p_0p_1\cdots$, where for simplicity we assume n is square-free, and $p_0>p_1>\cdots$. By sieve methods it can be shown that for most primes p, the prime divisors of $p-1$ have the same "nice" distribution. If $p_0,p_1,\ldots$ are such "normal" primes, it follows that $\phi(n)=(p_0-1)(p_1-1)\cdots$ has about $\log_2 n-\log_2 p_1$ prime factors in $[p_1,n]$, about $2(\log_2 p_1-\log_2 p_2)$ prime factors in $[p_2,p_1]$, and in general, $\phi(n)$ will have $k(\log_2 p_{k-1}-\log_2 p_k)$ prime factors in $[p_k,p_{k-1}]$. That is, n has k times as many prime factors in the interval $[p_k,p_{k-1}]$ as does a "normal" integer of its size. If n has many "large" prime divisors, then the prime factors of $m=\phi(n)$ will be much denser than normal, and the number, N_1, of such integers m will be "small". On the other hand, the number, N_2 of integers n with relatively few "large" prime factors is also "small". Our objective then is to precisely define these concepts of "large" and "small" so as to minimize N_1+N_2.

The argument in [26] is based on the heuristic that a normal totient is generated from a number n satisfying

$$\log_2 q_i(n)\approx\varrho^i\log_2 x \tag{1.10}$$

for each i (compare with (1.8)). As an alternative to this heuristic, assuming all prime factors of a pre-image n of a totient are normal leads to consideration of a series of inequalities among the prime factors of n. We show that such n generate "most" totients. By mapping the L largest prime factors of n (excluding the largest) to a point in $\mathbb{R}^L$, the problem of counting the number of such $n\leqslant x$ reduces to the problem of finding the volume of a certain region of $\mathbb{R}^L$, which we call the fundamental simplex. Our result is roughly

$$V(x)\approx\frac{x}{\log x}\max_L T_L(\log_2 x)^L,$$

where T_L denotes the volume of the simplex. It turns out that the maximum occurs at $L=L_0(x)+O(1)$. Careful analysis of these inequalities reveals that "most" of the integers n for which they are satisfied satisfy (1.8). Thus, the heuristic (1.10) gives numbers n for which the smaller prime factors are slightly too large. The crucial observation that the Lth largest prime factor ($L=L_0-1$) satisfies $\log_2 p_L\approx\frac{1}{L}\varrho^L\log_2 x$ is a key to determining the true order of $V(x)$.

In Section 2 we define "normal" primes and show that most primes are "normal". The set of linear inequalities used in the aforementioned heuristic are defined and analyzed in Section 3. The principal result is a determination of the volume of the simplex defined by the inequalities, which requires excursions into linear algebra and complex analysis. Section 4 is devoted to proving the upper bound for $V(x)$, and in section 5, the lower bound for $V_k(x)$ is deduced. Together these bounds establish Theorems 1 and 2, as well as Theorems 4, 5 and 8 as corollaries. The distribution of the prime factors of a pre-image of a typical totient are detailed in Section 6, culminating in the proof of Theorems 10–12 and Corollary 13.

In Section 7, we summarize the computations giving Theorem 6, present very elementary proofs of Theorems 7 and 9, prove Theorem 3 and discuss other problems about $V(x;k)$. Lastly, Section 8 outlines an extension of all of these results to more general multiplicative arithmetic functions such as $\sigma(n)$, the sum of divisors function. Specifically, we prove

Theorem 14. *Suppose $f:\mathbb{N}\to\mathbb{N}$ is a multiplicative function satisfying*

$$\{f(p)-p : p \textit{ prime}\} \textit{ is a finite set not containing 0,} \tag{1.11}$$

$$\sum_{h \textit{ square-full}} \frac{h^\delta}{f(h)} \ll 1, \qquad \textit{for some } \delta>0. \tag{1.12}$$

Then the analogs of Theorems 1–4, 8, 10–13 and 16 hold with $f(n)$ replacing $\phi(n)$, with the exception of the dependence on d in Theorems 2 and 8, which may be different.

Some functions appearing in the literature which satisfy the conditions of Theorem 14 are $\sigma(n)$, the sum of divisors function, $\phi^*(n)$, $\sigma^*(n)$ and $\psi(n)$. Here $\phi^*(n)$ and $\sigma^*(n)$ are the unitary analogs of $\phi(n)$ and $\sigma(n)$, defined by $\phi^*(p^k)=p^k-1$ and $\sigma^*(p^k)=p^k+1$ [6], and $\psi(n)$ is Dedekind's function, defined by $\psi(p^k)=p^k+p^{k-1}$. Now consider, for fixed $a\ne 0$, the function defined by $f(p^k)=(p+a)^k$ for $p\geqslant p_0 := \min\{p : p+a\geqslant 2\}$ and $f(p^k)=(p_0+a)^k$ for $p<p_0$. Then the range of f is the multiplicative semigroup generated by the shifted primes $p+a$ for $p>1-a$.

Corollary 15. *For a fixed nozero a, let $V^{(a)}(x)$ be the counting function of the multiplicative semigroup generated by the shifted primes $\{p+a : p+a\geqslant 2\}$. Then*

$$V^{(a)}(x) \asymp_a \frac{x}{\log x}\exp\{C(\log_3 x-\log_4 x)^2 + D\log_3 x - (D+1/2-2C)\log_4 x\}.$$

One further theorem, Theorem 16, depends on the definition of the fundamental simplex, and is not stated until Section 6.

Acknowledgement: The author is grateful to Paul Pollack for carefully proofreading of the manuscript and for catching a subtle error in the proof of the lower bound in Theorem 1.

2 Preliminary lemmata

Let $P^+(n)$ denote the largest prime factor of n and let $\Omega(n,U,T)$ denote the total number of prime factors p of n such that $U<p\leqslant T$, counted according to multiplicity. Constants implied by the Landau O and Vinogradov $\ll$ and $\gg$ symbols are absolute unless otherwise specified, and $c_1,c_2,\dots$ will denote absolute constants, not depending on any parameter. Symbols in boldface type indicate vector quantities.

A small set of additional symbols will have constant meaning throughout this paper. These include the constants $\mathscr{V}$, ϱ, C, D, a_i, defined respectively in (1.1), (1.4), (1.5), (1.6), and (1.3), as well as the constants $\mathscr{S}_L$, T_L, g_i and g_i^*, defined in section 3. Also included are the following functions: the functions defined in (1.1), $L_0(x)$ (1.7), $F(x)$ (1.3); the functions $Q(\alpha)$ and $W(x)$ defined respectively in Lemma 2.1 and (2.5) below; and $\mathscr{S}_L(\boldsymbol{\xi})$, $T_L(\boldsymbol{\xi})$, $\mathscr{R}_L(\boldsymbol{\xi};x)$, $R_L(\boldsymbol{\xi};x)$ and $x_i(n;x)$ defined in section 3. Other variables are considered "local" and may change meaning from section to section, or from lemma to lemma.

A crucial tool in the proofs of Theorems 1 and 2 is a more precise version of the result from [26] that for most primes p, the larger prime factors of $p-1$ are nicely distributed (see Lemma 2.6 below). We begin with three basic lemmas.

Lemma 2.1. *If $z > 0$ and $0 < \alpha < 1 < \beta$ then*

$$\sum_{k \leqslant \alpha z} \frac{z^k}{k!} < e^{(1-Q(\alpha))z}, \qquad \sum_{k \geqslant \beta z} \frac{z^k}{k!} < e^{(1-Q(\beta))z},$$

where $Q(\lambda) = \int_1^\lambda \log t\, dt = \lambda \log(\lambda) - \lambda + 1$.

Proof. We have

$$\sum_{k \leqslant \alpha z} \frac{z^k}{k!} = \sum_{k \leqslant \alpha z} \frac{(\alpha z)^k}{k!} \left(\frac{1}{\alpha}\right)^k \leqslant \left(\frac{1}{\alpha}\right)^{\alpha z} \sum_{k \leqslant \alpha z} \frac{(\alpha z)^k}{k!} < \left(\frac{e}{\alpha}\right)^{\alpha z} = e^{(1-Q(\alpha))z}.$$

The second inequality follows in the same way. □

Lemma 2.2. *The number of integers $n \leqslant x$ for which $\Omega(n) \geqslant \alpha \log_2 x$ is*

$$\ll_\alpha \begin{cases} x(\log x)^{-Q(\alpha)} & 1 < \alpha < 2 \\ x(\log x)^{1-\alpha \log 2} \log_2 x & \alpha \geqslant 2. \end{cases}$$

Proof. This can be deduced from the Theorems in Chapter 0 of [20]. □

Lemma 2.3. *The number of $n \leqslant x$ divisible by a number $m \geqslant \exp\{(\log_2 x)^2\}$ with $P^+(m) \leqslant m^{2/\log_2 x}$ is $\ll x/\log^2 x$.*

Proof. Let $\Psi(x, y)$ denote the number of integers $\leqslant x$ which have no prime factors $> y$. For x large, standard estimates ([23], Theorem 1.1 and Corollary 2.3) give

$$\Psi(z, z^{2/\log_2 x}) \ll z \exp\{-(\log_2 x \log_3 x)/3\}$$

uniformly for $z \geqslant \exp\{(\log_2 x)^2\}$. The lemma follows by partial summation. □

We also need basic sieve estimates ([19], Theorems 4.1, 4.2).

Lemma 2.4. *Uniformly for $1.9 \leqslant y \leqslant z \leqslant x$, we have*

$$|\{n \leqslant x : p|n \implies p \notin (y, z]\}| \ll x \frac{\log y}{\log z}.$$

Lemma 2.5. *Suppose $a_1, \dots, a_h$ are positive integers and $b_1, \dots, b_h$ are integers such that*

$$E = \prod_{i=1}^{h} a_i \prod_{1 \leqslant i < j \leqslant h} (a_i b_j - a_j b_i) \neq 0.$$

Then

$$\#\{n \leqslant x : a_i n + b_i \text{ prime } (1 \leqslant i \leqslant h)\} \ll_h \frac{x(\log_2(|E| + 10))^h}{(\log z)^h}.$$

Next, we examine the normal multiplicative structure of shifted primes $p - 1$.

Definition 1. *When $S \geqslant 2$, a prime p is said to be S-normal if*

$$\Omega(p - 1, 1, S) \leqslant 2 \log_2 S \tag{2.1}$$

and, for every pair of real numbers (U, T) with $S \leqslant U < T \leqslant p - 1$, we have

$$|\Omega(p - 1, U, T) - (\log_2 T - \log_2 U)| < \sqrt{\log_2 S \log_2 T}. \tag{2.2}$$

We remark that (2.1) and (2.2) imply that for an S-normal prime $p \geqslant S$,

$$\Omega(p - 1) \leqslant 3 \log_2 p. \tag{2.3}$$

This definition is slightly weaker than, and also simpler than, the definition of S-normal given in [14].

Lemma 2.6. *Uniformly for $x \geqslant 3$ and $S \geqslant 2$, the number of primes $p \leqslant x$ which are not S-normal is*

$$\ll \frac{x(\log_2 x)^5}{\log x}(\log S)^{-1/6}.$$

Proof. Assume x is sufficiently large and $S \geqslant \log^{1000} x$, otherwise the lemma is trivial. Also, if $\log S > (\log x)^6$, then (2.1) implies that the number of p in question is

$$\leqslant x \sum_{n \leqslant x} \frac{(3/2)^{\Omega(n)-2\log_2 S}}{n} \ll x\frac{(\log x)^{3/2}}{(\log S)^{2\log(3/2)}} \ll \frac{x}{(\log x)(\log S)^{0.3}}.$$

Next, assume $\log S \leqslant (\log x)^6$. By Lemmas 2.2 and 2.3, the number of primes $p \leqslant x$ with either $p < \sqrt{x}$, $q := P^+(p-1) \leqslant x^{2/\log_2 x}$, $\Omega(p-1) \geqslant 10\log_2 x$ or $p-1$ divisible by the square of a prime $\geqslant S$, is $O(x/\log^2 x)$. Let p be a prime not in these categories, which is also not S-normal. Write $p-1 = qb$. By (2.1) and (2.2), either (i) $\Omega(b,1,S) \geqslant 2\log_2 S - 1$ or (ii) for some $S \leqslant U < T \leqslant x$, $|\Omega(b,U,T) - (\log_2 T - \log_2 U)| \geqslant \sqrt{\log_2 S \log_2 T} - 1$. By Lemma 2.5, for each b, the number of q is

$$\ll \frac{x}{\phi(b)\log^2(x/b)} \ll \frac{x(\log_2 x)^3}{b\log^2 x}.$$

If $S \leqslant x$, the sum of $1/b$ over b satisfying (i) is

$$\leqslant \sum_{\substack{P^+(b')\leqslant S \\ \Omega(b')\geqslant 2\log_2 S-1}} \frac{1}{b'} \prod_{S<p\leqslant x}\left(1+\frac{1}{p}\right) \ll \frac{\log x}{\log S}\left(\frac{3}{2}\right)^{1-2\log_2 S} \sum_{P^+(b')\leqslant S} \frac{(3/2)^{\Omega(b')}}{b'}$$
$$\ll (\log x)(\log S)^{1/2-2\log(3/2)} \ll (\log x)(\log S)^{-0.3},$$

and otherwise the sum is

$$\leqslant \sum_{\substack{b'\leqslant x \\ \Omega(b')\geqslant 2\log_2 S-1}} \frac{1}{b'} \ll \left(\frac{3}{2}\right)^{1-2\log_2 S} \sum_{b'\leqslant x} \frac{(3/2)^{\Omega(b')}}{b'} \ll \frac{(\log x)^{3/2}}{(\log S)^{2\log(3/2)}} \ll \frac{\log x}{(\log S)^{0.3}}.$$

Consider b satisfying (ii). In particular, $S \leqslant x$. For positive integers k, let $t_k = e^{e^k}$. For some integers j,k satisfying $\log_2 S - 1 \leqslant j < k \leqslant \log_2 x + 1$, we have

$$|\Omega(b,t_j,t_k) - (k-j+1)| \geqslant \sqrt{(k-1)\log_2 S} - 4, \tag{2.4}$$

for otherwise if $t_j \leqslant U \leqslant t_{j+1}$ and $t_k \leqslant T < t_{k+1}$, then $\Omega(b,t_{j+1},t_k) \leqslant \Omega(b,U,T) \leqslant \Omega(b,t_j,t_{k+1})$, implying (2.2). Now fix j,k and let $h = \sqrt{(k-1)\log_2 S} - 4$. For any integer $l \geqslant 0$,

$$\sum_{\Omega(b,t_j,t_k)=l} \frac{1}{b} \leqslant \prod_{p\leqslant t_j}\left(1+\frac{1}{p}\right) \prod_{t_k<p\leqslant x}\left(1+\frac{1}{p}\right)\frac{1}{l!}\left(\sum_{t_j<p\leqslant t_k}\frac{1}{p}\right)^l \ll e^{j-k}\log x\,\frac{(k-j+1)^l}{l!}.$$

Summing over $|l-(k-j+1)| \geqslant h$ using Lemma 2.1, we see that for each pair (j,k), there are

$$\ll \frac{x(\log_2 x)^3}{\log x} e^{-(k-j)Q(\beta)}$$

primes satisfying (ii), where $\beta = 1 + \frac{h}{k-j+1}$. Here we used the fact that $Q(1-\lambda) > Q(1+\lambda)$ for $0 < \lambda \leqslant 1$. By the integral representation of $Q(x)$, we have $Q(1+\lambda) \geqslant \frac{\lambda}{2}\log(1+\lambda)$. Also, $h \geqslant 0.99\sqrt{k\log_2 S} \geqslant 990$. If $h \geqslant k-j+1$, then

$$(k-j)Q(\beta) \geqslant \frac{h(k-j)\log 2}{2(k-j+1)} \geqslant \frac{h\log 2}{4} \geqslant \frac{\log_2 S}{6},$$

and if $h < k - j + 1$, then

$$(k-j)Q(\beta) \geqslant \frac{(k-j)\log 2}{2}\left(\frac{h}{k-j+1}\right)^2 \geqslant \frac{h^2}{3(k-j+1)} \geqslant \frac{\log_2 S}{4}.$$

As there are $\leqslant (\log_2 x)^2$ choices for the pair (j,k), the proof is complete. □

Lemma 2.7. *There are $O(\frac{x\log_2 x}{Y})$ numbers $m \in \mathscr{V}(x)$ with either m or some $n \in \phi^{-1}(m)$ divisible by d^2 for some $d > Y$.*

Proof. If $\phi(n) \leqslant x$, then from a standard estimate, $n \ll x\log_2 x$. Now $\sum_{d>Y} z/d^2 \ll z/Y$. □

Our next result says roughly that most totients have a preimage which is S-normal for an appropriate S, and that neither the totient nor preimage has a large square factor or a large number of prime factors.

Definition 2. *A totient m is said to be S-nice if*

(a) *$\Omega(m) \leqslant 5\log_2 m$,*
(b) *$d^2|m$ or $d^2|n$ for some $n \in \phi^{-1}(m)$ implies $d \leqslant S^{1/2}$,*
(c) *for all $n \in \phi^{-1}(m)$, n is divisible only by S-normal primes.*

Now let

$$W(x) = \max_{2\leqslant y\leqslant x} \frac{V(y)\log y}{y}. \tag{2.5}$$

Lemma 2.8. *Uniformly for $x \geqslant 3$ and $2 \leqslant S \leqslant x$, the number of $m \in \mathscr{V}(x)$ which are not S-nice is*

$$O\left(\frac{xW(x)(\log_2 x)^6}{\log x}(\log S)^{-1/6}\right).$$

Proof. We may suppose $S \geqslant \exp\{(\log_2 x)^{36}\}$, for otherwise the lemma is trivial. By Lemmas 2.2 and 2.7, the number of totients failing (a) or failing (b) is $O(x/\log^2 x)$. Suppose p is a prime divisor of n for some $n \in \phi^{-1}(m)$. If $n = n'p$ then either $\phi(n) = (p-1)\phi(n')$ or $\phi(n) = p\phi(n')$, so in either case $\phi(n') \leqslant x/(p-1)$. Let $G(t)$ denote the number of primes $p \leqslant t$ which are not S-normal. By Lemma 2.6, the number of m failing (c) is at most

$$\begin{aligned}2\sum_p V\left(\frac{x}{p-1}\right) &\ll \sum_p \frac{xW(x/(p-1))}{(p-1)\log(x/p)} \\ &\ll xW(x)\int_2^{x/2}\frac{G(t)dt}{t^2\log(x/t)} \ll \frac{xW(x)(\log_2 x)^6}{\log x}(\log S)^{-1/6}.\end{aligned}$$ □

3 The fundamental simplex

For a natural number n, write $n = q_1q_2\cdots$, where $q_1 \geqslant q_2 \geqslant \cdots$, q_i are prime for $i \leqslant \Omega(n)$ and $q_i = 1$ for $i > \Omega(n)$. For $\mathscr{S} \subseteq [0,1]^L$, let $\mathscr{R}_L(\mathscr{S}; y)$ denote the set of integers n with $\Omega(n) \leqslant L$ and

$$\left(\frac{\max(0,\log_2 q_i)}{\log_2 y}, \ldots, \frac{\max(0,\log_2 q_L)}{\log_2 y}\right) \in \mathscr{S},$$

where $\max(0,\log_2 1)$ is defined to be 0. Also set

$$R_L(\mathscr{S}; y) = \sum_{n\in\mathscr{R}_L(\mathscr{S};y)} \frac{1}{\phi(n)}. \tag{3.1}$$

Heuristically, $R_L(\mathscr{S};x) \approx (\log_2 y)^L \operatorname{Vol}(\mathscr{S})$. Our result in this direction relates $R_L(\mathscr{S};y)$ to the volume of perturbations of $\mathscr{S}$. Specifically, letting $\mathscr{S}+\mathbf{v}$ denote the translation of $\mathscr{S}$ by the vector $\mathbf{v}$, for $\varepsilon>0$ let

$$\mathscr{S}^{+\varepsilon} = \bigcup_{\mathbf{v}\in[-\varepsilon,\varepsilon]^L} (\mathscr{S}+\mathbf{v}), \qquad \mathscr{S}^{-\varepsilon} = \bigcap_{\mathbf{v}\in[-\varepsilon,\varepsilon]^L} (\mathscr{S}+\mathbf{v}).$$

Lemma 3.1. *Let $y \geqslant 2000$, $\varepsilon = 1/\log_2 y$ and suppose $\mathscr{S} \subseteq \{\mathbf{x}\in\mathbb{R}^L : 0 \leqslant x_L \leqslant \cdots \leqslant x_1 \leqslant 1\}$. Then*

$$(\log_2 y)^L \operatorname{Vol}\left(\mathscr{S}^{-\varepsilon}\right) \ll R_L(\mathscr{S};y) \ll (\log_2 y)^L \operatorname{Vol}\left(\mathscr{S}^{+\varepsilon}\right).$$

Proof. For positive integers $m_1,\ldots,m_L$, let $B(\mathbf{m}) = \prod_{i=1}^L [(m_i-1)\varepsilon, m_i\varepsilon)$. If $\mathscr{B}$ is the set of boxes $B(\mathbf{m})$ entirely contained in $\mathscr{S}$, then the union of these boxes contains $\mathscr{S}^{-\varepsilon}$. Moreover, for each box, $m_1 > m_2 > \ldots > m_L \geqslant 1$. For $m \geqslant 1$, there is at least one prime in $I_m := [\exp(e^{m-1}), \exp(e^m))$, thus

$$\begin{aligned} R_L(\mathscr{S};y) &\geqslant \sum_{B(\mathbf{m})\in\mathscr{B}} \prod_{i=1}^L \sum_{m_i-1\leqslant \log_2 p < m_i} \frac{1}{p-1} \\ &= \sum_{B(\mathbf{m})\in\mathscr{B}} \prod_{i=1}^L \max\left(\exp\{-e^{m_i}\}, 1+O(e^{-m_i})\right) \gg |\mathscr{B}| \geqslant (\log_2 y)^L \operatorname{Vol}(\mathscr{S}^{-\varepsilon}). \end{aligned}$$

For the second part, suppose $\mathscr{S}$ is nonempty and let $\mathscr{B}$ be the set of boxes $B(\mathbf{m})$ which intersect $\mathscr{S}$, so that their union is contained in $\mathscr{S}^{+\varepsilon}$. For $B(\mathbf{m})\in\mathscr{B}$, let $j_m = |\{i : m_i = m\}|$. Then

$$R_L(\mathscr{S};y) \leqslant \sum_{B(\mathbf{m})\in\mathscr{B}} \prod_{m\geqslant 1} U(m,j_m), \qquad U(m,j) = \sum_{r_1\leqslant\cdots\leqslant r_j, r_i\in I_m} \frac{1}{\phi(r_1\cdots r_j)}.$$

Here each r_i is prime, except that when $m=0$ we allow $r_i=1$ also. We have $U(0,j) \leqslant \sum_{P^+(n)\leqslant 13} 1/\phi(n) \ll 1$. Now suppose $m \geqslant 1$ and let $j = j_m$. For each $r_1,\ldots,r_j$, write $r_1\cdots r_j = kh$, where $(k,h)=1$, k is squarefree and h is squarefull. Also let $\ell = \omega(k)$. Setting

$$t_m = \sum_{\substack{h \text{ squarefull} \\ p|h \implies p\in I_m}} \frac{1}{\phi(h)}, \qquad s_m = \sum_{p\in I_m} \frac{1}{p-1} = 1+O(e^{-m}),$$

we have

$$U(m,j) \leqslant \frac{s_m^j}{j!} + t_m \sum_{\ell=0}^{j-2} \frac{s_m^\ell}{\ell!} \leqslant \frac{s_m^j}{j!} + t_m e^{s_m} \leqslant 1+O(e^{-m}).$$

We conclude that

$$R_L(\mathscr{S};y) \ll \sum_{B(\mathbf{m})\in\mathscr{B}} \prod_{m\geqslant 1} (1+O(e^{-m})) \ll |\mathscr{B}| \leqslant (\log_2 y)^L \operatorname{Vol}(\mathscr{S}^{+\varepsilon}). \qquad \square$$

Suppose $\xi_i > 0$ for $0 \leqslant i \leqslant L-1$. Recall (1.3) and let $\mathscr{S}_L^*(\boldsymbol{\xi})$ be the set of $(x_1,\ldots,x_L)\in\mathbb{R}^L$ satisfying

$$\begin{aligned} &(I_0) && a_1x_1 + a_2x_2 + \cdots + a_Lx_L \leqslant \xi_0, \\ &(I_1) && a_1x_2 + a_2x_3 + \cdots + a_{L-1}x_L \leqslant \xi_1 x_1, \\ &\vdots && \vdots \\ &(I_{L-2}) && a_1x_{L-1} + a_2x_L \leqslant \xi_{L-2}x_{L-2}, \\ &(I_{L-1}) && 0 \leqslant x_L \leqslant \xi_{L-1}x_{L-1}. \end{aligned}$$

and let $\mathscr{S}_L(\boldsymbol{\xi})$ be the subset of $\mathscr{S}_L^*(\boldsymbol{\xi})$ satisfying $0 \leqslant x_L \leqslant \cdots \leqslant x_1 \leqslant 1$. Define

$$T_L^*(\boldsymbol{\xi}) = \operatorname{Vol}(\mathscr{S}_L^*(\boldsymbol{\xi})), \qquad T_L(\boldsymbol{\xi}) = \operatorname{Vol}(\mathscr{S}_L(\boldsymbol{\xi})).$$

For convenience, let $\mathbf{1} = (1, 1, \dots, 1)$, $\mathscr{S}_L = \mathscr{S}_L(\mathbf{1})$ (the "fundamental simplex"), $T_L = \mathrm{Vol}(\mathscr{S}_L)$, $\mathscr{S}_L^* = \mathscr{S}_L^*(\mathbf{1})$, and $T_L^* = \mathrm{Vol}(\mathscr{S}_L^*)$. We first relate $\mathscr{S}_L(\boldsymbol{\xi})$ to $\mathscr{S}_L$. The next lemma is trivial.

Lemma 3.2. *If $\xi_i \geqslant 1$ for all i, and $\mathbf{x} \in \mathscr{S}_L(\boldsymbol{\xi})$, then $\mathbf{y} \in \mathscr{S}_L$, where $y_i = (\xi_0 \cdots \xi_{i-1})^{-1} x_i$. If $0 < \xi_i \leqslant 1$ for all i and $\mathbf{y} \in \mathscr{S}_L$, then $\mathbf{x} \in \mathscr{S}_L(\boldsymbol{\xi})$, where $x_i = (\xi_0 \cdots \xi_{i-1}) y_i$.*

Corollary 3.3. *Define $H(\boldsymbol{\xi}) = \xi_0^L \xi_1^{L-1} \cdots \xi_{L-2}^2 \xi_{L-1}$. We have $T_L \leqslant T_L(\boldsymbol{\xi}) \leqslant H(\boldsymbol{\xi}) T_L$ when $\xi_i \geqslant 1$ for all i, and $H(\boldsymbol{\xi}) T_L \leqslant T_L(\boldsymbol{\xi}) \leqslant T_L$ when $0 < \xi_i \leqslant 1$ for all i.*

In applications, $H(\boldsymbol{\xi})$ will be close to 1, so we concentrate on bounding T_L.

Lemma 3.4. *We have*

$$T_L^* \asymp T_L \asymp \frac{\varrho^{L(L+3)/2}}{L!} (F'(\varrho))^L.$$

Corollary 3.5. *If $H(\boldsymbol{\xi}) \asymp 1$, then*

$$T_L(\boldsymbol{\xi}) \asymp T_L(\boldsymbol{\xi}) \asymp \frac{\varrho^{L(L+3)/2}}{L!} (F'(\varrho))^L.$$

Furthermore, if $L = 2C(\log_3 x - \log_4 x) - \Psi$, where $0 \leqslant \Psi \ll \sqrt{\log_3 x}$, then

$$\begin{aligned}(\log_2 x)^L T_L(\boldsymbol{\xi}) = \exp\{&C(\log_3 x - \log_4 x)^2 + D \log_3 x - (D + 1/2 - 2C) \log_4 x \\ &- \Psi^2/4C - (D/2C - 1)\Psi + O(1)\}.\end{aligned}$$

If $L = [2C(\log_3 x - \log_4 x)] - \Psi > 0$, then

$$\begin{aligned}(\log_2 x)^L T_L(\boldsymbol{\xi}) \ll \exp\{&C(\log_3 x - \log_4 x)^2 + D \log_3 x - (D + 1/2 - 2C) \log_4 x \\ &- \Psi^2/4C - (D/2C - 1)\Psi\}.\end{aligned}$$

Proof. The second and third parts follow from (1.5), (1.6) and Stirling's formula. □

To prove Lemma 3.4, we first give a variant of a standard formula for the volume of tetrahedra, then an asymptotic for a sequence which arises in the proof.

Lemma 3.6. *Suppose $\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_L \in \mathbb{R}^L$, any L of which are linearly independent, and*

$$\mathbf{v}_0 + \sum_{i=1}^{L} b_i \mathbf{v}_i = \mathbf{0}, \tag{3.2}$$

where $b_i > 0$ for every i. Also suppose $\alpha > 0$. The volume, V, of the simplex

$$\{\mathbf{x} \in \mathbb{R}^L : \mathbf{v}_i \cdot \mathbf{x} \leqslant 0 \, (1 \leqslant i \leqslant L), \mathbf{v}_0 \cdot \mathbf{x} \leqslant \alpha\}$$

is

$$V = \frac{\alpha^L}{L!(b_1 b_2 \cdots b_L) |\det(\mathbf{v}_1, \dots, \mathbf{v}_L)|}.$$

Proof. We may assume that $\alpha = b_1 = b_2 = \cdots = b_L = 1$, for the general case follows by suitably scaling the vectors $\mathbf{v}_i$. The vertices of the simplex are $\mathbf{0}, \mathbf{p}_1, \cdots, \mathbf{p}_L$, where $\mathbf{p}_i$ satisfies

$$\begin{cases} \mathbf{p}_i \cdot \mathbf{v}_j = 0 \quad (1 \leqslant j \leqslant L, j \neq i); \\ \mathbf{p}_i \cdot \mathbf{v}_0 = 1. \end{cases}$$

Taking the dot product of $\mathbf{p}_i$ with each side of (3.2) yields $\mathbf{v}_i \cdot \mathbf{p}_i = -1$, so $\mathbf{p}_i$ lies in the region $\{\mathbf{v}_i \cdot \mathbf{x} \leqslant 0\}$. Also, $\mathbf{0}$ lies in the half-plane $\mathbf{v}_0 \cdot \mathbf{x} \leqslant \alpha$. The given region is thus an L-dimensional "hyper-tetrahedron" with volume $|\det(\mathbf{p}_1, \cdots, \mathbf{p}_L)|/L!$, and $(\mathbf{p}_1, \cdots, \mathbf{p}_L)(\mathbf{v}_1, \cdots, \mathbf{v}_L)^T = -I$, where I is the identity matrix. Taking determinants gives the lemma. □

Having $2L-2$ inequalities defining $\mathscr{S}_L$ creates complications estimating T_L, so we devise a scheme where only $L+1$ inequalities are considered at a time, thus allowing the use of Lemma 3.6. The numbers b_i occurring in that lemma will come from the sequence $\{g_i\}$, defined by

$$g_0 = 1, \qquad g_i = \sum_{j=1}^{i} a_j g_{i-j} \quad (i \geqslant 1). \tag{3.3}$$

Lemma 3.7. *For every $i \geqslant 1$, $|g_i - \lambda\varrho^{-i}| \leqslant 5$, where $\lambda = \frac{1}{\varrho F'(\varrho)}$.*

Proof. Write $1 - F(z) = (1 - z/\varrho) l(z)$ and $l(z) = \sum_{n=0}^{\infty} l_n z^n$. By (1.4),

$$l_n = \varrho^{-m}\left(1 - \sum_{k=1}^{n} a_k \varrho^k\right) = \sum_{k=1}^{\infty} \varrho^k a_{n+k} > 0.$$

Next consider $k(z) = (1-z)^2 l(z) = \sum_{n=0}^{\infty} k_n z^n$. We have $k_0 = 1$, $k_1 = l_1 - 2 = \varrho^{-1} - a_1 - 2 < 0$ and

$$k_n = l_n - 2l_{n-1} + l_{n-2} = \sum_{k=1}^{\infty} \varrho^k \left(a_{n+k} - 2a_{n+k-1} + a_{n+k-2}\right) < 0 \qquad (n \geqslant 2).$$

Also, $k_n = O(1/n^2)$, and $\sum_{n\geqslant 1} k_n = -1$. Thus, $k(z)$ is analytic for $|z| < 1$, continuous on $|z| \leqslant 1$, and nonzero for $|z| \leqslant 1, z \neq 1$. Further,

$$\Re k(z) \geqslant 1 + k_1 \Re z - (1 + k_1) = |k_1| \Re(1 - z),$$

so that for $|z| < 1$,

$$\left|\frac{1}{l(z)}\right| \leqslant \frac{|1-z|^2}{|k_1|\Re(1-z)} \leqslant \frac{1}{|k_1|} \max_{|z|=1} \frac{|1-z|^2}{\Re(1-z)} = \frac{2}{|k_1|} < 3.7.$$

Now let

$$e(z) = \sum_{n=0}^{\infty} \left(g_n - \lambda\varrho^{-i}\right) z^n = \frac{1}{1-F(z)} - \frac{\lambda}{1 - z/\varrho} = \frac{1/l(z) - 1/l(\varrho)}{1 - z/\varrho}.$$

From the preceding arguments, we see that $e(z)$ is analytic for $|z| < 1$ and continuous on $|z| \leqslant 1$. By the maximum modulus principle, $\max_{|z|=1} |e(z)| \leqslant (3.7 + \lambda)/|1/\varrho - 1| \leqslant 5$. By Cauchy's integral formula, the Taylor coefficients of $e(z)$ are all bounded by 5 in absolute value. □

Remark 1. The above proof is based on [17], and is much simpler than the original proof given in [14]. With more work, one can show that for $i \geqslant 1$, the numbers $g_i - \lambda\varrho^{-i}$ are negative, increasing and have sum $-1 + \lambda/(1-\varrho) = -0.2938\ldots$

Proof of Lemma 3.4. The basic idea is that $\mathscr{S}_L^*$ is only slightly larger than $\mathscr{S}_L$. In other words, the inequalities $1 \geqslant x_1 \geqslant \cdots \geqslant x_{L-1}$ are relatively insignificant. Set

$$\mathscr{U}_0 = \mathscr{S}_L^* \cap \{x_1 > 1\}, \qquad \mathscr{U}_i = \mathscr{S}_L^* \cap \{x_i < x_{i+1}\} \quad (1 \leqslant i \leqslant L-2)$$

and $V_i = \mathrm{Vol}(\mathscr{U}_i)$. Evidently

$$T_L^* - \sum_{i=0}^{L-2} V_i \leqslant T_L \leqslant T_L^*. \tag{3.4}$$

Let $\mathbf{e}_1, \cdots, \mathbf{e}_L$ denote the standard basis for $\mathbb{R}^L$, i.e. $\mathbf{e}_i \cdot \mathbf{x} = x_i$. For $1 \leqslant i \leqslant L-2$, set

$$\mathbf{v}_i = -\mathbf{e}_i + \sum_{j=1}^{L-i} a_j \mathbf{e}_{i+j} \tag{3.5}$$

and also

$$\mathbf{v}_0 = \sum_{j=1}^{L} a_j \mathbf{e}_j, \qquad \mathbf{v}_{L-1} = -\mathbf{e}_{L-1} + \mathbf{e}_L, \qquad \mathbf{v}_L = -\mathbf{e}_L.$$

For convenience, define

$$g_0^* = 1, \quad g_i^* = g_i + (1-a_1)g_{i-1} \qquad (i \geqslant 1). \tag{3.6}$$

Thus, for $1 \leqslant j \leqslant L-2$, inequality (I_j) may be abbreviated as $\mathbf{v}_j \cdot \mathbf{x} \leqslant 0$. Also, inequality (I_0) is equivalent to $\mathbf{v}_0 \cdot \mathbf{x} \leqslant 1$ and (I_{L-1}) is represented by $\mathbf{v}_{L-1} \cdot \mathbf{x} \leqslant 0$ and $\mathbf{v}_L \cdot \mathbf{x} \leqslant 0$. By (3.3), (3.5) and (3.6),

$$\mathbf{e}_i = -\sum_{j=i}^{L-1} g_{j-i}\mathbf{v}_j - g_{L-i}^* \mathbf{v}_L. \tag{3.7}$$

It follows that

$$\mathbf{v}_0 + \sum_{j=1}^{L-1} g_j \mathbf{v}_j + g_L^* \mathbf{v}_L = \mathbf{0}. \tag{3.8}$$

Since $|\det(\mathbf{v}_1, \cdots, \mathbf{v}_L)| = 1$, Lemma 3.6 and (3.8) give

$$T_L^* = \frac{1}{L!(g_1 \cdots g_{L-1})g_L^*}. \tag{3.9}$$

Lemma 3.7 now implies the claimed estimate for T_L^*.

For the remaining argument, assume L is sufficiently large. We shall show that

$$\sum_{i=0}^{L-2} V_i < 0.61 T_L^*, \tag{3.10}$$

which, combined with (3.4), (3.9) and Lemma 3.7, proves Lemma 3.4.

Combining $x_1 \geqslant 1$ with $\mathbf{v}_0 \cdot \mathbf{x} \leqslant 1$ gives $\mathbf{u} \cdot \mathbf{x} \leqslant 0$, where $\mathbf{u} = \mathbf{v}_0 - \mathbf{e}_1$. By (3.7) and (3.8),

$$\mathbf{u} = \sum_{j=1}^{L-1} (g_{j-1} - g_j)\mathbf{v}_j + (g_{L-1}^* - g_L^*)\mathbf{v}_L.$$

Thus

$$\mathbf{v}_0 + \frac{a_1}{1-a_1}\mathbf{u} + \sum_{j=2}^{L} b_j \mathbf{v}_j = \mathbf{0},$$

where

$$\begin{aligned} b_j &= g_j + \frac{a_1}{1-a_1}(g_j - g_{j-1}) \qquad (2 \leqslant j \leqslant L-1), \\ b_L &= g_L^* + \frac{a_1}{1-a_1}(g_L^* - g_{L-1}^*). \end{aligned}$$

Lemma 3.7 implies $b_j > (9/7)g_j$ for large j, In addition, $|\det(\mathbf{u}, \mathbf{v}_2, \ldots, \mathbf{v}_L)| = (1-a_1)$. By Lemma 3.6,

$$V_0 \ll \frac{1}{L!(b_2 b_3 \cdots b_L)} \ll \left(\frac{7}{9}\right)^L T_L^*. \tag{3.11}$$

We next show that

$$V_i = \frac{1}{(1-a_1)L!(g_1 \cdots g_{i-1})A_i B_i} \prod_{j=i+2}^{L-1} \left(\frac{1}{g_j + B_i h_{j-i}} \right) \frac{1}{g_L^* + B_i h_{L-i}^*}, \tag{3.12}$$

where

$$A_i = g_i + \frac{g_{i+1}}{1-a_1}, \quad B_i = \frac{g_{i+1}}{1-a_1}, \quad h_l = g_l - g_{l-1}, \quad h_l^* = h_l + (1-a_1)h_{l-1}.$$

In $\mathscr{U}_i$ we have (I_i) and $x_i \leqslant x_{i+1}$, hence

$$x_{i+1} \geqslant \frac{1}{1-a_1}(a_2x_{i+2} + \cdots + a_{L-i}x_L) \geqslant x_{i+2} + a_2x_{i+3} + \cdots + a_{L-i-1}x_L.$$

The condition $\mathbf{v}_{i+1} \cdot \mathbf{x} \leqslant 0$ is therefore implied by the other inequalities defining $\mathscr{U}_i$, which means

$$V_i = \mathrm{Vol}\{\mathbf{v}_0 \cdot \mathbf{x} \leqslant 1; \mathbf{v}_j \cdot \mathbf{x} \leqslant 0 \ (1 \leqslant j \leqslant L, j \neq i+1); (\mathbf{e}_i - \mathbf{e}_{i+1}) \cdot \mathbf{x} \leqslant 0\}.$$

We note $|\det(\mathbf{v}_1, \cdots, \mathbf{v}_i, \mathbf{e}_i - \mathbf{e}_{i+1}, \mathbf{v}_{i+2}, \cdots, \mathbf{v}_L)| = (1-a_1)$. It is also easy to show from (3.8) that

$$\mathbf{0} = \mathbf{v}_0 + \sum_{j=1}^{i-1} g_j\mathbf{v}_j + A_i\mathbf{v}_i + B_i(\mathbf{e}_i - \mathbf{e}_{i+1}) + \sum_{j=i+2}^{L} b_j\mathbf{v}_j,$$

where $b_j = g_j + B_ih_{j-i}$ for $i+2 \leqslant j \leqslant L-1$, and $b_L = g_L^* + B_ih_{L-i}^*$. An application of Lemma 3.6 completes the proof of (3.12).

We now deduce numerical estimates for V_i/T_L^*. Using Lemma 3.7, plus explicit computation of g_i for small i, gives $A_i > 4$ for all i and

$$\begin{aligned} g_j + B_ih_{j-i} &> 1.44g_j \qquad (i \text{ large, say } i \geqslant L-100),\\ g_j + B_ih_{j-i} &> 1.16g_j \qquad (i \geqslant 1, j \geqslant i+2),\\ g_L^* + B_ih_{L-i}^* &> 1.44g_L^* \qquad (i < L-2),\\ g_L^* + B_{L-2}h_2^* &> 1.19g_L^*. \end{aligned}$$

From these bounds, plus (3.9) and (3.12), it follows that

$$\begin{aligned} V_{L-2}/T_L^* &< (4 \cdot 1.19)^{-1},\\ V_i/T_L^* &< (4 \cdot 1.44^{L-i-1})^{-1} \qquad (L-99 \leqslant i \leqslant L-3),\\ V_i/T_L^* &< (4 \cdot 1.44^{99} \cdot 1.16^{L-i-100})^{-1} \qquad (1 \leqslant i \leqslant L-100). \end{aligned}$$

Combining these bounds with (3.11) yields

$$\sum_{i=0}^{L-2} V_i/T_L^* < O((4/5)^L) + \frac{1}{4}\left(\frac{1}{1.19} + \frac{1.44^{-2}}{1-1.44^{-1}} + \frac{1.44^{-99}}{(1-1/1.16)}\right) < 0.61,$$

which implies (3.10). This completes the proof of Lemma 3.4. □

Important in the study of $\mathscr{S}_L$ and $\mathscr{S}_L^*$ are both global bounds on the numbers x_i (given below) as well as a determination of where “most” of the volume lies (given below in Lemma 3.10 Section 6).

Lemma 3.8. *Let $x_0 = 1$. If $\mathbf{x} \in \mathscr{S}_L^*$, then $x_i \geqslant g_{j-i}x_j$ for $0 \leqslant i \leqslant j \leqslant L$. If $\mathbf{x} \in \mathscr{S}_L(\boldsymbol{\xi})$ and $\xi_i \geqslant 1$ for all i, then $x_j \leqslant 4.771\xi_i \cdots \xi_{j-1}\varrho^{j-i}x_i$ for $0 \leqslant i < j \leqslant L$.*

Proof. Fix i and note that the first inequality is trivial for $j = i$. Assume $k \leqslant i-2$ and it holds for $j \geqslant k+1$. Then by (I_k) and the induction hypothesis,

$$x_k \geqslant \sum_{h=1}^{L-k} a_hx_{k+h} \geqslant \sum_{h=1}^{i-k} a_hg_{i-k-h}x_i = g_{i-k}x_i.$$

By Lemma 3.7, the maximum of ϱ^{-i}/g_i is $4.7709\ldots$, occurring at $i = 2$. The second inequality follows by Lemma 3.2. □

Careful analysis of $\mathscr{S}_L$ reveals that most of the volume occurs with $x_i \approx \frac{L-i}{L}\varrho^i$ for each i, with the "standard deviation" from the mean increasing with i. This observation plays an important role in subsequent arguments. For now, we restrict our attention to the variable x_L, which will be useful in estimating sums over numbers n, whose L largest prime factors lie in a specific set, and whose other prime factors are unconstrained. Results concerning the size of x_i for $i < L$ will not be needed until section 6.

Lemma 3.9. *Let $L \geqslant 3$, $\alpha \geqslant 2\varepsilon > 0$ and $\xi_i \geqslant 1$ for each i. If $\mathbf{x} \in [\mathscr{S}_L^*(\boldsymbol{\xi}) \cap \{x_L \geqslant \alpha\}]^{+\varepsilon}$, then $\mathbf{y} \in \mathscr{S}_L^* \cap \{y_L \geqslant \alpha'\}$, where $\alpha' = (\alpha-\varepsilon)/(\xi_0'\cdots\xi_{L-1}')$, $\xi_{L-1}' = 3\xi_{L-1}$ and for $1 \leqslant i \leqslant L-2$,*

$$y_i = \frac{x_i}{\xi_0'\cdots\xi_{i-1}'}, \qquad \xi_i' = \xi_i\left(1 + \frac{10\varrho^{L-i}(1+a_1+\cdots+a_{L-i})\xi_0\cdots\xi_{L-1}}{\alpha/\varepsilon}\right).$$

Proof. By assumption, for some $\mathbf{x}' \in \mathscr{S}_L^*(\boldsymbol{\xi})$ with $x_L' \geqslant \alpha$, $|x_i - x_i'| \leqslant \varepsilon$ for all i. By Lemma 3.8,

$$x_i \geqslant x_i' - \varepsilon \geqslant \frac{x_i'}{2} \geqslant \frac{\varrho^{i-L}x_L'}{10\xi_1\cdots\xi_{L-1}} \geqslant \frac{\varrho^{i-L}\alpha}{10\xi_0\cdots\xi_{L-1}} \qquad (i \leqslant L-1).$$

Hence, by (I_i), if $i \leqslant L-2$ then

$$\begin{aligned}\sum_{j=1}^{L-i} a_j x_{i+j} &\leqslant \sum_{j=1}^{L-i} a_j(x_{i+j}'+\varepsilon) \leqslant \xi_i x_i' + \varepsilon(a_1+\cdots+a_{L-i}) \\ &\leqslant \xi_i(x_i + \varepsilon(a_1+\cdots+a_{L-i})) \leqslant \xi_i' x_i.\end{aligned}$$

Lastly,

$$x_{L-1} \geqslant x_{L-1}' - \varepsilon \geqslant \xi_{L-1}^{-1}x_L' - \varepsilon \geqslant \xi_{L-1}^{-1}\max(\varepsilon, x_L - 2\varepsilon) \geqslant \frac{x_L}{3\xi_{L-1}} = \frac{x_L}{\xi_{L-1}'}.$$

This shows that $\mathbf{x} \in \mathscr{S}_L^*(\boldsymbol{\xi}')$ and $x_L \geqslant \alpha - \varepsilon$. Finally, by Lemma 3.2, $\mathbf{y} \in \mathscr{S}_L^*$ and $y_L \geqslant \alpha'$. □

The next lemma shows that $x_L \approx \varrho^L/L$ for most of $\mathscr{S}_L$, significantly smaller than the global upper bound given by Lemma 3.8.

Lemma 3.10. *(i) If $\alpha \geqslant 0$, then*

$$\mathrm{Vol}(\mathscr{S}_L^* \cap \{x_L \leqslant \alpha\}) \ll T_L \alpha L \varrho^{-L}$$

and

$$\mathrm{Vol}(\mathscr{S}_L^* \cap \{x_L \geqslant \alpha\}) \ll e^{-\alpha L g_L} T_L.$$

(ii) If $\alpha \geqslant 0$, $\xi_i \geqslant 1$ for each i, $H(\boldsymbol{\xi}) \leqslant 2$ and $\varepsilon \leqslant 10\varrho^L/L$, then

$$\mathrm{Vol}([\mathscr{S}_L^*(\boldsymbol{\xi}) \cap \{x_L \geqslant \alpha\}]^{+\varepsilon}) \ll e^{-C_0\alpha L g_L} T_L$$

for some absolute constant $C_0 > 0$.

Proof. Consider first $\mathbf{x} \in \mathscr{S}_L^* \cap \{x_L \leqslant \alpha\}$. Since $(x_1,\ldots,x_{L-1}) \in \mathscr{S}_{L-1}^*$, the volume is $\leqslant \alpha T_{L-1}^*$. Applying Lemma 3.4 gives the first part of (i). Next, suppose $\mathbf{x} \in \mathscr{S}_L^* \cap \{x_L \geqslant \alpha\}$. If $\alpha \geqslant 1/g_L$, the volume is zero by Lemma 3.8. Otherwise, set $y_i = x_i - \alpha g_{L-i}$ for each i. We have $y_{L-1} \geqslant y_L \geqslant 0$, $\mathbf{v}_j \cdot \mathbf{y} \leqslant 0$ for $1 \leqslant j \leqslant L-2$, and $\mathbf{v}_0 \cdot \mathbf{y} \leqslant 1 - \alpha g_L$. By Lemmas 3.4 and 3.6, the volume of such $\mathbf{y}$ is $\leqslant (1-\alpha g_L)^L T_L^* \ll (1-\alpha g_L)^L T_L$. The second part of (i) now follows.

For (ii), first suppose $\alpha \geqslant 2\varepsilon$. By Lemma 3.9, Corollary 3.3 and part (i),

$$\mathrm{Vol}([\mathscr{S}_L^*(\boldsymbol{\xi}) \cap \{x_L \geqslant \alpha\}]^{+\varepsilon}) \leqslant H(\boldsymbol{\xi}')\,\mathrm{Vol}(\mathscr{S}_L^* \cap \{y_L \geqslant \alpha'\}) \ll T_L e^{-\alpha' L g_L},$$

where α' is defined in Lemma 3.9. Since $H(\boldsymbol{\xi}) \leqslant 2$, $H(\boldsymbol{\xi}') \ll 1$ and hence $\alpha' \gg \alpha$. Next, assume $\alpha < 2\varepsilon$. Without loss of generality suppose $\alpha = 0$, since $e^{-2\varepsilon L g_L} \gg 1$ by Lemma 3.7, (3.6) and the assumed upper bound on ε. For $\mathbf{x}$ in question, let $r = \max\{i \leqslant L : x_i \geqslant 2\varepsilon\}$. Using Lemma 3.4 and part (i),

$$\begin{aligned} \mathrm{Vol}([\mathscr{S}_L^*(\boldsymbol{\xi}) \cap \{x_L \geqslant \alpha\}]^{+\varepsilon}) &\ll \sum_{r=0}^{L} (2\varepsilon)^{L-r}\,\mathrm{Vol}\left(\mathscr{S}_r^*((\xi_0, \ldots, \xi_{r-1}))\right) \\ &\ll T_L \sum_{h=0}^{L} (2\varepsilon)^h \left(\frac{T_{L-h}}{T_L}\right) \ll T_L \sum_{h=0}^{L} \left(\frac{2\varepsilon L \varrho^{10-L}}{F'(\varrho)}\right)^h \ll T_L. \qquad \square \end{aligned}$$

4 The upper bound for $V(x)$

In this section, we prove that

$$V(x) \ll \frac{xZ(x)}{\log x}, \quad Z(x) = \exp\{C(\log_3 x - \log_4 x)^2 + D(\log_3 x) - (D + 1/2 - 2C)\log_4 x\}. \tag{4.1}$$

We begin with the basic tools needed for the proof, which show immediately the significance of the set $\mathscr{S}_L(\boldsymbol{\xi})$. First, recall the definition of an S-normal prime (2.1)–(2.2). Also, factor each positive integer

$$n = q_0(n)q_1(n)\cdots, \quad q_0(n) \geqslant q_1(n) \geqslant \cdots,$$

$q_i(n)$ is prime for $i < \Omega(n)$ and $q_i(n) = 1$ for $i \geqslant \Omega(n)$. Define

$$x_i(n; x) = \frac{\max(0, \log_2 q_i(n))}{\log_2 x}. \tag{4.2}$$

Lemma 4.1. *Suppose y is sufficiently large, $k \geqslant 2$ and*

$$1 \geqslant \theta_1 \geqslant \cdots \geqslant \theta_k \geqslant \frac{\log_2 S}{\log_2 y},$$

where $S \geqslant \exp\{(\log_2 y)^{36}\}$. Let $\log_2 E_j = \theta_j \log_2 y$ for each j. The number of S-nice totients $v \leqslant y$ with a pre-image satisfying

$$q_j(n) \geqslant E_j \qquad (1 \leqslant j \leqslant k)$$

is

$$\ll y(\log y)^{A+B}(\log_2 y)(\log S)^{k \log k} + \frac{y}{(\log y)^2},$$

where

$$A = -\sum_{j=1}^{k} a_j \theta_j, \qquad B = 4\sqrt{\frac{\log_2 S}{\log_2 y}} \sum_{j=2}^{k+1} \theta_{j-1}^{1/2} j \log j.$$

Proof. Let $F = \min(E_1, y^{1/(20 \log_2 y)})$, $E_{k+1} = S$, and $\theta_{k+1} = \log_2 S / \log_2 y$. Let m be the part of v composed of primes in $(S, F]$. Then $m \leqslant F^{\Omega(v)} \leqslant y^{1/2}$. By Lemma 2.4, the number of totients with a given m is

$$\ll \frac{y}{m} \frac{\log S}{\log F} \leqslant \frac{y}{m} (\log y)^{\theta_{k+1} - \theta_1} (\log_2 y).$$

Let

$$\delta_j = \frac{\sqrt{\log_2 S \log_2 E_{j-1}}}{\log_2 y}$$

for each j. Since the primes $q_i(n)$ are S-normal, by (2.2)

$$\Omega(m, E_j, E_{j-1}) \geqslant j(\theta_{j-1} - \theta_j - \delta_j)\log_2 y =: R_j \qquad (2 \leqslant j \leqslant k+1).$$

Therefore, the total number, N, of totients counted satisfies

$$N \ll y(\log y)^{\theta_{k+1}-\theta_1}(\log_2 y)\prod_{j=2}^{k+1}\sum_{r\geqslant R_j}\frac{t_j^r}{r!},$$

where

$$t_j = \sum_{E_j<p\leqslant E_{j-1}}\frac{1}{p}\leqslant(\theta_{j-1}-\theta_j)\log_2 y+1 := s_j.$$

If $\delta_j\leqslant\frac{1}{2}(\theta_{j-1}-\theta_j)$, then

$$\frac{s_j}{R_j}\leqslant\frac{1}{j}\left(1+\frac{3\delta_j}{\theta_{j-1}-\theta_j}\right)$$

and Lemma 2.1 implies

$$\begin{aligned}\sum_{r\geqslant R_j}\frac{s_j^r}{r!}\leqslant\left(\frac{es_j}{R_j}\right)^{R_j} &\leqslant(\log y)^{j(\theta_{j-1}-\theta_j-\delta_j)(1-\log j+3\delta_j/(\theta_{j-1}-\theta_j))}\\ &\leqslant(\log y)^{(j-j\log j)(\theta_{j-1}-\theta_j)+(j\log j+2j)\delta_j}.\end{aligned}$$

If $\delta_j>\frac{1}{2}(\theta_{j-1}-\theta_j)$, then the sum on r is

$$\leqslant e^{s_j}\leqslant e(\log y)^{(j-j\log j)(\theta_{j-1}-\theta_j)+(2j\log j)\delta_j}.$$

Therefore,

$$N\ll y(\log y)^{A+B}(\log_2 y)(\log S)^{(k+1)\log(k+1)-k}e^k.$$

□

Lemma 4.2. *Recall definitions* (1.3). *Suppose* $k\geqslant 2$, $0<\omega<1/10$ *and* y *is sufficiently large (say* $y\geqslant y_0$*). Then the number of totients* $v\leqslant y$ *with a pre-image* n *satisfying*

$$a_1x_1(n;y)+\cdots+a_kx_k(n;y)\geqslant 1+\omega$$

is

$$\ll y(\log_2 y)^6W(y)(\log y)^{-1-\omega^2/(600k^3\log k)}.$$

Proof. Assume that

$$\omega^2>3600\frac{\log_3 y}{\log_2 y}k^3\log k, \tag{4.3}$$

for otherwise the lemma is trivial. Define S by

$$\log_2 S=\frac{\omega^2}{100k^3\log k}\log_2 y, \tag{4.4}$$

so that $S\geqslant\exp\{(\log_2 y)^{36}\}$. Let $U(y)$ denote the number of totients in question which are S-nice. By (4.4) and Lemma 2.8, the number of totients not counted by $U(y)$ is

$$\ll\frac{y(\log_2 y)^6W(y)}{\log y}(\log S)^{-1/6}+\frac{y\log_2 y}{S}\ll y(\log_2 y)^6W(y)(\log y)^{-1-\omega^2/(600k^3\log k)}.$$

Let $\varepsilon=\omega/10$, $\alpha=a_1+\cdots+a_k<k\log k$, and suppose n is a pre-image of a totient counted in $U(y)$. Let $x_i=x_i(n;y)$ for $1\leqslant i\leqslant k$. Then there are numbers $\theta_1,\ldots,\theta_k$ so that $\theta_i\leqslant x_i$ for each i, each θ_i is an integral multiple of ε/α, $\theta_1\geqslant\cdots\geqslant\theta_k$, and

$$1+\omega-\varepsilon\leqslant a_1\theta_1+\cdots+a_k\theta_k\leqslant 1+\omega. \tag{4.5}$$

For each admissible k-tuple $\boldsymbol{\theta}$, let $T(\boldsymbol{\theta}; y)$ denote the number of totients counted in $U(y)$ which have some pre-image n satisfying $x_i(n; y) \geqslant \theta_i$ for $1 \leqslant i \leqslant k$. Let j be the largest index with $\theta_j \geqslant \log_2 S/\log_2 y$. By Lemma 4.1,

$$T(\boldsymbol{\theta}; y) \ll y(\log y)^{A+B}(\log_2 y)(\log S)^{k\log k} + y(\log y)^{-2},$$

where, by (4.5),

$$A = -\sum_{i=1}^{j} a_i\theta_i \leqslant -(1+0.9\omega) + \alpha\frac{\log_2 S}{\log_2 y}$$

and, by (4.4), (4.5) and the Cauchy-Schwartz inequality,

$$B \leqslant 4\left(\frac{\log_2 S}{\log_2 y}(1+\omega)\sum_{j=2}^{k+1}\frac{j^2\log^2 j}{a_{j-1}}\right)^{1/2} \leqslant 6\left(\frac{k^3\log k\log_2 S}{\log_2 y}\right)^{1/2} \leqslant \frac{3\omega}{5}.$$

Also

$$(\log S)^{2k\log k} = (\log y)^{\omega^2/(50k^2)} \leqslant (\log y)^{\omega/2000}.$$

Using (4.3), the number of vectors $\boldsymbol{\theta}$ is trivially at most

$$\left(\frac{\alpha}{\varepsilon}\right)^k \leqslant \left(\frac{10k\log k}{\omega}\right)^k \leqslant (\log_2 y)^{k/2} \leqslant (\log y)^{\omega^2/3000} \leqslant (\log y)^{\omega/30000}.$$

Therefore,

$$U(y) \leqslant \sum_{\boldsymbol{\theta}} T(\boldsymbol{\theta}; y) \ll y(\log y)^{-1-\omega/4},$$

which finishes the proof. □

Before proceeding with the main argument, we prove a crude upper bound for $V(x)$ to get things started using the method of Pomerance [29]. For a large x let $x' \leqslant x$ be such that $V(x') = x'W(x)/\log x'$. Let $v \leqslant x'$ be a totient with pre-image n. By Lemma 2.7, the number of v with $p^2|n$ for some prime $p > e^{\sqrt{\log x'}}$ is $O(x'/\log x')$. By Lemma 4.2, the number of v with $a_1x_1(n; x') + a_2x_2(n; x') > 1.01$ is $O(x'W(x')(\log x')^{-1-c})$ for some $c > 0$. On the other hand, if $a_1x_1(n; x') + a_2x_2(n; x') \leqslant 1.01$, then $x_2(n; x') \leqslant 0.8$. Write $v = \phi(q_0q_1)m$, so that $m \leqslant \exp\{(\log x')^{0.8}\}$, $p_0^2 \nmid n$ and $p_1^2 \nmid n$. Therefore,

$$W(x) \ll 1 + \frac{W(x)}{(\log x')^c} + \sum_{q_1}\sum_{m}\frac{1}{(q_1-1)m} \ll (\log_2 x)^2 W(\exp\{(\log x)^{0.8}\}).$$

Iterating this inequality yields

$$W(x) \ll \exp\{9(\log_3 x)^2\}. \tag{4.6}$$

Lemma 4.3. *We have*

$$\sum_{\substack{v\in\mathscr{V}\\ P^+(v)\leqslant y}} \frac{1}{v} \ll W(y^{\log_2 y})\log_2 y \ll \exp\{10(\log_3 y)^2\}.$$

Proof. Let $f(z)$ denote the number of totients $v \leqslant z$ with $P^+(v) \leqslant y$, and set $y' = y^{\log_2 y}$. First suppose $z \geqslant y'$. If $v > z^{1/2}$, then $P^+(v) < v^{2/\log_2 y}$, so Lemma 2.3 gives $f(z) \ll z/\log^2 z$. For $z < y'$, use the trivial bound $f(z) \leqslant V(z)$. The lemma follows from $\log_2 y' = \log_2 y + \log_3 y$, (4.6) and partial summation. □

Proof of (4.1). Let $L = L_0(x)$ and for $0 \leqslant i \leqslant L-1$, let

$$\omega_i = \frac{1}{10000} \exp\left\{ -\frac{L-i}{40} \right\}, \qquad \xi_i = 1 + \omega_i. \tag{4.7}$$

Then $H(\boldsymbol{\xi}) \leqslant 1.1$. Let v be a generic totient $\leqslant x$ with a pre-image n satisfying $n \geqslant x/\log x$ and $\Omega(n) \leqslant 10\log_2 x$, and set $x_i = x_i(n;x)$ and $q_i = q_i(n)$ for $i \geqslant 0$. By Lemma 2.2,

$$V(x) \leqslant \sum_{j=0}^{L-2} M_j(x) + N(x) + O\left(\frac{x}{\log x}\right),$$

where $M_j(x)$ denotes the number of such totients $\leqslant x$ with a pre-image satisfying inequality (I_i) for $i < j$ but not satisfying inequality (I_j), and $N(x)$ denotes the number of such totients with every pre-image satisfying $\mathbf{x} \in \mathscr{S}_L(\boldsymbol{\xi})$. By Lemma 4.2 (with $\omega = \omega_0$) and (4.6), $M_0(x) \ll x/\log x$. Now suppose $1 \leqslant j \leqslant L-2$, and set $k = L - j$. Let n be a pre-image of a totient counted in $M_j(x)$, and set $w = q_j q_{j+1} \cdots, m = \phi(w)$. Since ($I_0$) holds, $x_2 \leqslant \xi_0/(a_1+a_2) < 0.9$. It follows that $q_0 > x^{1/3}$, whence $m < x^{2/3}$. By the definition of $M_j(x)$ and (4.7),

$$x_j \leqslant \xi_j^{-1}(a_1 x_{j+1} + a_2 x_{j+2} + \cdots) < \xi_{j-1}^{-1}(a_1 x_j + a_2 x_{j+1} + \cdots) \leqslant x_{j-1},$$

whence $q_{j-1} > q_j$ and $\phi(n) = \phi(q_0 \cdots q_{j-1})m$. For each m, the number of choices for $q_0, \ldots, q_{j-1}$ is

$$\ll \frac{x}{m \log x} R_{j-1}(\mathscr{S}_{j-1}(\xi_0, \ldots, \xi_{j-3}); x),$$

where we set $\mathscr{S}_0 = \{0\}$, $\mathscr{S}_1 = [0,1]$ and $\mathscr{S}_2 = [0,1]^2$. Let $f(y)$ be the number of $m \leqslant y$. Define Y_j by $\log_3 Y_j = k/20 + 1000$. Since m is a totient, we have $f(y) \leqslant V(y)$, but when $y > Y_j$ we can do much better. First note that $w \ll y \log_2 y$. By Lemma 2.3, the number of such w with $P^+(w) < y^{1/\log_2 y}$ is $O(y/(\log y)^3)$. Otherwise, we have $q_j = P^+(w) \geqslant y^{1/\log_2 y}$ and

$$x_j \geqslant \frac{\log_2 y - \log_3 y}{\log_2 x} \geqslant \frac{\log_2 y}{\log_2 x}\left(1 - \frac{k/20+1000}{e^{k/20+1000}}\right).$$

For $0 \leqslant i \leqslant k$, let

$$z_i = x_i(w; y) = \frac{\log_2 x}{\log_2 y} x_{i+j}.$$

Since (I_j) fails and $y > Y_j$, it follows that

$$a_1 z_1 + \cdots + a_k z_k \geqslant \frac{\log_2 x}{\log_2 y}(1+\omega_j) x_j \geqslant (1 + \omega_j/2).$$

By Lemma 4.2 and (4.6), when $y \geqslant \max(y_0, Y_j)$ we have

$$f(y) \ll \frac{yW(y)(\log_2 y)^6}{\log y} \exp\left\{ -\frac{\omega_j^2}{600k^3 \log k} \log_2 y \right\} \ll \frac{y}{\log y (\log_2 y)^2}.$$

By partial summation and Lemma 4.3,

$$\sum_m \frac{1}{m} \ll 1 + \sum_{m \leqslant Y_j} \frac{1}{m} \ll W(Y_j) \log_2 Y_j \ll \exp\{k^2/40 + O(k)\}.$$

Therefore, by Lemma 3.1, Corollary 3.5 (with $\Psi = k+1$) and Lemma 3.10 (ii) with $\alpha = 0$,

$$\begin{aligned} M_j(x) &\ll \frac{x}{\log x} R_{j-1}(\mathscr{S}_{j-1}(\xi_0,\ldots,\xi_{j-1});x)\exp\{k^2/40\} \\ &\ll \frac{x}{\log x} T_{j-1}(\log_2 x)^{j-1}\exp\{k^2/40\} \\ &\ll \frac{x}{\log x}\exp\{-k^2/4-((D+1)/2C-1)k\}Z(x). \end{aligned} \tag{4.8}$$

Thus

$$\sum_{j=0}^{L-1} M_j(x) \ll \frac{x}{\log x} Z(x). \tag{4.9}$$

Next, suppose n is a pre-image of a totient counted in $N(x)$. By Lemma 3.8, $x_L \leqslant 5\varrho^L \leqslant \frac{20\log_3 x}{\log_2 x}$. If b is a nonnegative integer, let $N_b(x)$ be the number of totients counted in $N(x)$ with a pre-image $n > x/\log^2 x$ satisfying $b/\log_2 x \leqslant x_L \leqslant (b+1)/\log_2 x$. Let $w = q_{L+1}\cdots$ and $q = q_1\cdots q_L w$. Since $x_2 < 0.9$ we have $q < x^{2/3}$. As $\phi(q) \geqslant \phi(q_1\cdots q_L)\phi(w)$, for a fixed q the number of possibilities for q_0 is

$$\ll \frac{x}{\log x}\frac{1}{\phi(q)} \leqslant \frac{x}{\log x}\frac{1}{\phi(q_1\cdots q_L)v}, \; v = \phi(w).$$

By Lemma 3.1 and Lemma 3.10 (ii),

$$\sum \frac{1}{\phi(q_1\cdots q_L)} \ll R_L(\mathscr{S}_L(\boldsymbol{\xi}) \cap \{x_L \geqslant b/\log_2 x\};x) \ll Z(x)e^{-C_0 b/4}.$$

By Lemma 4.3 and (4.6), $\sum \frac{1}{v} \ll \exp\{10\log^2 b\}$. Combining these estimates gives

$$N_b(x) \ll \frac{x}{\log x} Z(x)\exp\{-C_0 b/4 + 10\log^2 b\}. \tag{4.10}$$

Summing on b gives $N(x) \ll \frac{x}{\log x}Z(x)$, which together with (4.9) gives (4.1). □

5 The lower bound for $V_\kappa(x)$

Our lower bound for $V_\kappa(x)$ is obtained by constructing a set of numbers with multiplicative structure similar to the numbers counted by $N(x)$ in the upper bound argument. At the core is the following estimate, which is proved using the lower bound method from [26].

Lemma 5.1. *Let y be large, $k \geqslant 1$, $e^e \leqslant S \leqslant v_k < u_{k-1} < v_{k-1} < u_{k-2} < \cdots < u_0 < v_0 = y$, $v_1 \leqslant y^{1/10\log_2 y}$, $l \geqslant 0$, $1 \leqslant r \leqslant y^{1/10}$, $\delta = \sqrt{\log_2 S/\log_2 y}$. Set $\nu_j = \log_2 v_j/\log_2 y$ and $\mu_j = \log_2 u_j/\log_2 y$ for each j. Suppose also that $\nu_{j-1} - \nu_j \geqslant 2\delta$ for $2 \leqslant j \leqslant k$, $1 \leqslant d \leqslant y^{1/100}$ and $P^+(d) \leqslant v_k$. The number of solutions of*

$$(p_0-1)\cdots(p_{k-1}-1)f_1\cdots f_l d = (q_0-1)\cdots(q_{k-1}-1)e \leqslant y/r, \tag{5.1}$$

in $p_0,\ldots,p_{k-1},f_1,\ldots,f_l,q_0,\ldots,q_{k-1},e$ satisfying

(1) *p_i and q_i are S-normal primes, neither $p_i - 1$ nor $q_i - 1$ is divisible by r^2 for a prime $r \geqslant v_k$;*

(2) *$p_i \neq q_i$ and $u_i \leqslant P^+(p_i-1), P^+(q_i-1) \leqslant v_i$ for $0 \leqslant i \leqslant k-1$;*

(3) *$P^+(ef_1\cdots f_l) \leqslant v_k$; $\Omega(f_i) \leqslant 10\log_2 v_k$ for all i;*

(4) *$p_0 - 1$ has a divisor $\geqslant y^{1/2}$ which is composed of primes $\geqslant v_1$;*

is

$$\ll \frac{y}{dr}(c_4\log_2 y)^{6k}(k+1)^{\Omega(d)}(\log v_k)^{20(k+l)\log(k+l)+1}(\log y)^{-2+\sum_{i=1}^{k-1}a_i\nu_i+E},$$

where c_4 is a positive constant and $E = \delta\sum_{i=2}^{k}(i\log i + i) + 2\sum_{i=1}^{k-1}(\nu_i - \mu_i)$.

Proof. We consider separately the prime factors of each shifted prime lying in each interval $(v_i, v_{i+1}]$. For $0 \leqslant j \leqslant k-1$ and $0 \leqslant i \leqslant k$, let

$$s_{i,j}(n) = \prod_{\substack{p^a \| (p_j - 1) \\ p \leqslant v_i}} p^a, \qquad s'_{i,j}(n) = \prod_{\substack{p^a \| (q_j - 1) \\ p \leqslant v_i}} p^a, \qquad s_i = df_1 \cdots f_l \prod_{j=0}^{k-1} s_{i,j} = e \prod_{j=0}^{k-1} s'_{i,j}.$$

Also, for $0 \leqslant j \leqslant k-1$ and $1 \leqslant i \leqslant k$, let

$$t_{i,j} = \frac{s_{i-1,j}}{s_{i,j}}, \qquad t'_{i,j} = \frac{s'_{i-1,j}}{s'_{i,j}}, \qquad t_i = \prod_{j=0}^{k-1} t_{i,j} = \prod_{j=0}^{k-1} t'_{i,j}.$$

For each solution $\mathscr{A} = (p_0, \ldots, p_{k-1}, f_1, \ldots, f_l, q_0, \ldots, q_{k-1}, e)$ of (5.1), let

$$\begin{aligned} \sigma_i(\mathscr{A}) &= \{s_i; s_{i,0}, \ldots, s_{i,k-1}, f_1, \ldots, f_l; s'_{i,0}, \ldots, s'_{i,k-1}, e\}, \\ \tau_i(\mathscr{A}) &= \{t_i; t_{i,0}, \ldots, t_{i,k-1}, 1, \ldots, 1; t'_{i,0}, \ldots, t'_{i,k-1}, 1\}. \end{aligned}$$

Defining multiplication of $(2k+l+2)$-tuples by component-wise multiplication, we have

$$\sigma_{i-1}(\mathscr{A}) = \sigma_i(\mathscr{A}) \tau_i(\mathscr{A}). \tag{5.2}$$

Let $\mathfrak{S}_i$ denote the set of $\sigma_i(\mathscr{A})$ arising from solutions $\mathscr{A}$ of (5.36) and $\mathfrak{T}_i$ the corresponding set of $\tau_i(\mathscr{A})$. By (5.2), the number of solutions of (5.1) satisfying the required conditions is

$$|\mathfrak{S}_0| = \sum_{\sigma \in \mathfrak{S}_1} \sum_{\substack{\tau \in \mathfrak{T}_1 \\ \sigma\tau \in \mathfrak{S}_0}} 1. \tag{5.3}$$

We will apply an iterative procedure based on the identity

$$\sum_{\sigma_{i-1} \in \mathfrak{S}_{i-1}} \frac{1}{s_{i-1}} = \sum_{\sigma_i \in \mathfrak{S}_i} \frac{1}{s_i} \sum_{\substack{\tau_i \in \mathfrak{T}_i \\ \sigma_i \tau_i \in \mathfrak{S}_{i-1}}} \frac{1}{t_i}. \tag{5.4}$$

First, fix $\sigma_1 \in \mathfrak{S}_1$. By assumption (4) in the lemma, $t_{1,0} \geqslant y^{1/2}$. Also, $t_1 = t_{1,0} = t'_{1,0} \leqslant y/(rs_1)$, t_1 is composed of primes $> v_1$, and also $s_{1,0}t_1 + 1$ and $s'_{1,0}t_1 + 1$ are different primes. Write $t_1 = t'_1 Q$, where $Q = P^+(t_1)$. Since $p_0 - 1$ is an S-normal prime, $Q \geqslant t_1^{1/\Omega(t_1)} \geqslant y^{1/6\log_2 y}$ by (2.3). Given t'_1, Lemma 2.5 implies that the number of Q is $O(y(\log_2 y)^6/(rs_1 t'_1 \log^3 y))$. Using Lemma 2.4 to bound the sum of $1/t'_1$, we have for each $\sigma_1 \in \mathfrak{S}_1$,

$$\sum_{\substack{\tau_1 \in \mathfrak{T}_1 \\ \sigma_1 \tau_1 \in \mathfrak{S}_0}} 1 \ll \frac{y(\log_2 y)^6}{rs_1(\log y)^{2+\nu_1}}. \tag{5.5}$$

Next, suppose $2 \leqslant i \leqslant k$, $\sigma_i \in \mathfrak{S}_i$, $\tau_i \in \mathfrak{T}_i$ and $\sigma_i\tau_i \in \mathfrak{S}_{i-1}$. By assumption (2),

$$t_i = t_{i,0} \cdots t_{i,i-1} = t'_{i,0} \cdots t'_{i,i-1}.$$

In addition, $s_{i,i-1}t_{i,i-1} + 1 = p_{i-1}$ and $s'_{i,i-1}t'_{i,i-1} + 1 = q_{i-1}$ are different primes. Let $Q_1 = P^+(t_{i,i-1})$, $Q_2 = P^+(t'_{i,i-1})$, $b = t_{i,i-1}/Q_1$ and $b' = t'_{i,i-1}/Q_2$.

We consider separately $\mathfrak{T}_{i,1}$, the set of τ_i with $Q_1 = Q_2$ and $\mathfrak{T}_{i,2}$, the set of τ_i with $Q_1 \neq Q_2$. First,

$$\Sigma_1 := \sum_{\substack{\tau_i \in \mathfrak{T}_{i,1} \\ \sigma_i \tau_i \in \mathfrak{S}_{i-1}}} \frac{1}{t_i} \leqslant \sum_t \frac{h(t)}{t} \max_{b,b'} \sum_{Q_1} \frac{1}{Q_1},$$

where $h(t)$ denotes the number of solutions of $t_{i,0}\cdots t_{i,i-2}b = t = t'_{i,0}\cdots t'_{i,i-2}b'$, and in the sum on Q_1, $s_{i,i-1}bQ_1+1$ and $s'_{i,i-1}b'Q_1+1$ are unequal primes. By Lemma 2.5, the number of $Q_1 \leqslant z$ is $\ll z(\log z)^{-3}(\log_2 y)^3$ uniformly in b, b'. By partial summation,

$$\sum_{Q_1 \geqslant u_{i-1}} \frac{1}{Q_1} \ll (\log_2 y)^3 (\log y)^{-2\mu_{i-1}}.$$

Also, $h(t)$ is at most the number of dual factorizations of t into i factors each, i.e. $h(t) \leqslant i^{2\Omega(t)}$. By (2.2), $\Omega(t) \leqslant i(\nu_{i-1}-\nu_i+\delta)\log_2 y =: I$. Also, by assumption (1), t is squarefree. Thus

$$\sum_t \frac{h(t)}{t} \leqslant \sum_{j \leqslant I} \frac{i^{2j}H^j}{j!},$$

where

$$\sum_{v_i < p \leqslant v_{i-1}} \frac{1}{p} \leqslant (\nu_{i-1}-\nu_i)\log_2 y + 1 =: H.$$

By assumption, $\nu_{i-1}-\nu_i \geqslant 2\delta$, hence $I \leqslant \frac{3}{2}iH \leqslant \frac{3}{4}i^2H$. Applying Lemma 2.1 (with $\alpha \leqslant \frac{3}{4}$) yields

$$\sum_t \frac{h(t)}{t} \leqslant \left(\frac{eHi^2}{I}\right)^I \leqslant (ei)^I = (\log y)^{(i+i\log i)(\nu_{i-1}-\nu_i+\delta)}. \tag{5.6}$$

This gives

$$\Sigma_1 \ll (\log_2 y)^3 (\log y)^{-2\mu_{i-1}+(i+i\log i)(\nu_{i-1}-\nu_i+\delta)}.$$

For the sum over $\mathfrak{T}_{i,2}$, set $t_i = tQ_1Q_2$. Note that

$$tQ_2 = t_{i,0}\cdots t_{i,i-2}b, \qquad tQ_1 = t'_{i,0}\cdots t'_{i,i-2}b',$$

so $Q_1 | t'_{i,0}\cdots t'_{i,i-2}b'$ and $Q_2 | t_{i,0}\cdots t_{i,i-2}b$. If we fix the factors divisible by Q_1 and by Q_2, then the number of possible ways to form t is $\leqslant i^{2\Omega(t)}$ as before. Then

$$\Sigma_2 := \sum_{\substack{\tau_i \in \mathfrak{T}_{i,2} \\ \sigma_i\tau_i \in \mathfrak{S}_{i-1}}} \frac{1}{t_i} \leqslant \sum_t \frac{i^{2\Omega(t)+2}}{t} \max_{b,b'} \sum_{Q_1,Q_2} \frac{1}{Q_1Q_2},$$

where $s_{i,i-1}bQ_1+1$ and $s'_{i,i-1}b'Q_2+1$ are unequal primes. By Lemma 2.5, the number of $Q_1 \leqslant z$ (respectively $Q_2 \leqslant z$) is $\ll z(\log z)^{-2}(\log_2 y)^2$. By partial summation, we have

$$\sum_{Q_1,Q_2} \frac{1}{Q_1Q_2} = \sum_{Q_1} \frac{1}{Q_1} \sum_{Q_2} \frac{1}{Q_2} \ll (\log_2 y)^4 (\log y)^{-2\mu_{i-1}}.$$

Combined with (5.6) this gives

$$\Sigma_2 \ll i^2 (\log_2 y)^4 (\log y)^{-2\mu_{i-1}+(i+i\log i)(\nu_{i-1}-\nu_i+\delta)}.$$

By assumption, $i^2 \leqslant k^2 \leqslant (\log_2 y)^2$. Adding Σ_1 and Σ_2 shows that for each σ_i,

$$\sum_{\substack{\tau_i \in \mathfrak{T}_i \\ \sigma_i\tau_i \in \mathfrak{S}_{i-1}}} \frac{1}{t_i} \ll (\log_2 y)^6 (\log y)^{-2\mu_{i-1}+(i\log i+i)(\nu_{i-1}-\nu_i+\delta)}. \tag{5.7}$$

Using (5.3) and (5.4) together with the inequalities (5.5) and (5.7), the number of solutions of (5.1) is

$$\ll \frac{y}{r}(c_4 \log_2 y)^{6k} (\log y)^{-2-\nu_1+\sum_{i=2}^k (\nu_{i-1}-\nu_i+\delta)(i\log i+i)-2\mu_{i-1}} \sum_{\sigma_k \in \mathfrak{S}_k} \frac{1}{s_k},$$

where c_4 is some positive constant. Note that the exponent of $(\log y)$ is $\leqslant -2+\sum_{i=1}^{k-1} a_i\nu_i + E$.

It remains to treat the sum on σ_k. Given $s_k' = s_k/d$, the number of possible σ_k is at most the number of factorizations of s_k' into $k+l$ factors times the number of factorizations of ds_k' into $k+1$ factors, which is at most $(k+1)^{\Omega(ds_k')}(k+l)^{\Omega(s_k')}$. By assumptions (1) and (3), $\Omega(s_k') \leqslant 10(k+l)\log_2 v_k$. Thus,

$$\sum_{\sigma_k\in\mathfrak{S}_k}\frac{1}{s_k}\leqslant \frac{(k+1)^{\Omega(d)}(k+l)^{20(k+l)\log_2 v_k}}{d}\sum_{P^+(s_k')\leqslant v_k}\frac{1}{s_k'} \ll \frac{(k+1)^{\Omega(d)}(\log v_k)^{20(k+l)\log(k+l)+1}}{d}. \qquad \square$$

Lemma 5.2. *If $\xi_i = 1-\omega_i$, $\omega_i = \frac{1}{10(L_0-i)^3}$ for each $i \leqslant L-2$, then there is an absolute constant M_1 so that whenever $1 \leqslant A \leqslant (\log y)^{1/2}$, $M = [M_1 + 2C\log A]$ and $L \leqslant L_0(y) - M$, we have*

$$R_L(\mathscr{S};y) \gg (\log_2 y)^L T_L, \tag{5.8}$$

where $\mathscr{S}$ is the subset of $\mathscr{S}_L(\boldsymbol{\xi})$ with the additional restrictions

$$x_{i+1} \leqslant (1-\omega_i)x_i \quad (i \geqslant 1), \qquad x_L \geqslant \frac{A}{\log_2 y}. \tag{5.9}$$

Proof. By Lemma 3.1, $R_L(\mathscr{S};y) \gg (\log_2 y)^L \operatorname{Vol}(\mathscr{S}^{-\varepsilon})$. For $1 \leqslant i \leqslant L-1$, put

$$\omega_i' = \frac{6(2+(L-i)\log(L-i))\varrho^{L-i}}{100+A}, \qquad \xi_i' = 1-\omega_i-\omega_i'.$$

Let $\mathscr{T}$ be the subset of $\mathscr{S}_L(\boldsymbol{\xi}')$ with the additional restrictions $x_{i+1} \leqslant \xi_i' x_i$ for each i and $x_L \geqslant (200+A)/\log_2 y$. Suppose $\mathbf{x} \in \mathscr{T}$ and $|x_i' - x_i| \leqslant \varepsilon$ for each i. By Lemma 3.8,

$$x_i' \geqslant \frac{x_i}{2} \geqslant \frac{\varrho^{L-i}}{6}x_L \geqslant \frac{\varrho^{L-i}(A+200)}{6\log_2 y}.$$

Thus, for $0 \leqslant i \leqslant L-1$,

$$x_{i+1}' \leqslant x_{i+1} + \varepsilon \leqslant \xi_i'(x_i' + \varepsilon) + \varepsilon \leqslant \left(\xi_i' + \frac{2\varepsilon}{x_i'}\right)x_i' \leqslant \xi_i x_i'$$

and

$$\begin{aligned} a_1 x_{i+1}' + \cdots + a_{L-i}x_L' &\leqslant \xi_i' x_i + \varepsilon(a_1 + \cdots a_{L-i}) \\ &\leqslant \xi_i'(x_i'+\varepsilon) + \varepsilon(1+(L-i)\log(L-i)) \leqslant \xi_i x_i'. \end{aligned}$$

Therefore, $\mathbf{x}' \in \mathscr{S}$ and hence $\mathscr{T} \subseteq \mathscr{S}^{-\varepsilon}$. Make the substitution $x_i = (\xi_0' \cdots \xi_{i-1}')y_i$ for $1 \leqslant i \leqslant L$. By Lemma 3.2, $\mathbf{y} \in \mathscr{T}' := \mathscr{S}_L \cap \{y_L \geqslant (A+200)/\log_2 y\}$. By Lemma 3.10 (i), if M_1 is large enough then

$$\operatorname{Vol}(\mathscr{S}^{-\varepsilon}) \geqslant \operatorname{Vol}(\mathscr{T}) \geqslant H(\boldsymbol{\xi}')\operatorname{Vol}(\mathscr{T}') \geqslant H(\boldsymbol{\xi}')\left[T_L - O(A\varrho^M T_L)\right] \gg T_L. \qquad \square$$

Now we proceed to the lower bound argument for Theorems 1 and 2. Suppose $A(d) = \kappa$ and $\phi(d_i) = d \quad (1 \leqslant i \leqslant \kappa)$. Assume throughout that $x \geqslant x_0(d)$. The variable k is reserved as an index for certain variables below. Define

$$M = M_2 + [(\log d)^{1/9}], M_2 \text{ is a sufficiently large absolute constant} \tag{5.10}$$

$$L = L_0(x) - M, \tag{5.11}$$

$$\xi_i = 1-\omega_i, \quad \omega_i = \frac{1}{10(L_0-i)^3} \qquad (0 \leqslant i \leqslant L-2). \tag{5.12}$$

Let $\mathscr{B}$ denote the set of integers $n = p_0p_1\cdots p_L > x^{9/10}$ with each p_i prime and

$$\phi(n) \leqslant x/d, \tag{5.13}$$

$$(x_1(n;x/d),\cdots,x_L(n;x/d)) \in \mathscr{S}_L(\boldsymbol{\xi}), \tag{5.14}$$

$$\log_2 p_i \geqslant (1+\omega_i)\log_2 p_{i+1} \qquad (0 \leqslant i \leqslant L-1), \tag{5.15}$$

$$p_L \geqslant \max(d+2, 17). \tag{5.16}$$

By Corollary 3.5 and Lemma 5.2 (with $y = x/d$, $A = \log_2 \max(d+2,17)$),

$$|\mathscr{B}| \gg \frac{x}{d\log(x/d)}(\log_2(x/d))^L T_L \gg \frac{x}{d\log x}(\log_2 x)^L T_L. \tag{5.17}$$

Consider the equation

$$d\phi(n) = \phi(n_1), \tag{5.18}$$

where $n \in \mathscr{B}$. Let $q_0 \geqslant q_1 \geqslant \cdots$ be the prime factors of n_1, and for $j \geqslant \Omega(n_1)$, put $q_j = 1$. If $n|n_1$, then none of the primes q_i $(0 \leqslant i \leqslant L)$ occur to a power greater than 1, for otherwise (5.16) gives $\phi(n_1) \geqslant \phi(n)p_L > \phi(n)d$. Also, $P^+(d_i) < p_L$ for all i. Therefore $\phi(n_1) = \phi(n_1/n)\phi(n) = \phi(n)d$, which implies $n_1 = nd_i$ for some i. These we will call the trivial solutions to (5.18). We then have $A(d\phi(n)) = \kappa$ for each $n \in \mathscr{B}$ for which (5.18) has no non-trivial solutions, i.e. solutions with $n \nmid n_1$. In particular, for such n we have $\phi(n') \neq \phi(n)$ for $n' \neq n$ and $n' \in \mathscr{B}$.

The numbers n which give rise to non-trivial solutions are grouped as follows. For $0 \leqslant j \leqslant L$, let $\mathscr{B}_j$ be the set of $n \in \mathscr{B}$ such that (5.18) holds for some n_1 with $q_i = p_i$ $(0 \leqslant i \leqslant j-1)$ and $p_j \neq q_j$, and such that (5.18) does not hold for any n_1 with $n \nmid n_1$ and $q_i = p_i$ $(0 \leqslant i \leqslant j)$. We then have

$$V_\kappa(x) \geqslant |\mathscr{B}| - \sum_{j=0}^{L} |\mathscr{B}_j|. \tag{5.19}$$

For $n \in \mathscr{B}_j$ with $j \geqslant 1$, write $n = p_0n_2n_3$, where $n_2 = p_1\cdots p_{j-1}$ and $n_3 = p_j\cdots p_L$. When $j = 0$, set $n_3 = n$. If $q_{j-1} = q_j$, then $p_{j-1}|d\phi(n_3)$, which is impossible. Therefore $q_{j-1} > q_j$ and $\phi(n_1) = \phi(p_0\cdots p_{j-1})\phi(q_j\cdots)$ and

$$d\phi(n_3) = \phi(n_4) \tag{5.20}$$

has a nontrivial solution n_4 (that is, with $n_3 \nmid n_4$). In addition, all such solutions satisfy $P^+(n_4) \neq P^+(n_3)$. Fix j and let $\mathscr{A}_j$ be the set of such n_3. It will be useful to associate a particular n_4 to each $n_3 \in \mathscr{A}_j$ as follows. Let $v = \phi(n_3)$ for some $n_3 \in \mathscr{A}_j$. If there is only one such n_3, then take n_4 to be the smallest nontrivial solution of (5.20). Otherwise, suppose there are exactly $k \geqslant 2$ members of $\mathscr{A}_j$, $n_{3,i}$ with $\phi(n_{3,i}) = v$ $(1 \leqslant i \leqslant k)$. Take a permutation σ of $\{1,\ldots,k\}$ with no fixed point and associate $n_4 = d_1n_{3,\sigma(i)}$ with $n_{3,i}$. Since $i \neq \sigma(i)$, $n_{3,i} \nmid n_4$, so the associated n_4 is a nontrivial solution of (5.20). In addition, distinct $n_3 \in \mathscr{A}_j$ are associated with distinct n_4.

For x large, (5.14) and (5.15) imply $p_0 > x^{3/4}$. By the prime number theorem, for each fixed n_2n_3, the number of choices for p_0 is $O(x/(d\phi(n_2n_3)\log x))$. Hence

$$|\mathscr{B}_j| \ll \frac{x}{d\log x}\sum_{n_2}\frac{1}{\phi(n_2)}\sum_{n_3}\frac{1}{\phi(n_3)} \quad (1 \leqslant j \leqslant L).$$

Since $n_2 \in \mathscr{R}_{j-1}(\mathscr{S}_{j-1};x)$ when $j \geqslant 2$, Lemma 5.2 gives

$$\sum_{n_2}\frac{1}{\phi(n_2)} \ll (\log_2 x)^{j-1}T_{j-1} \qquad (1 \leqslant j \leqslant L).$$

To attack the sum on n_3, let $B_j(y)$ denote the number of possible n_3 with $\phi(n_3) \leqslant y$. In particular, $|\mathscr{B}_0| = B_0(x/d)$. When $j \geqslant 1$, by partial summation,

$$|\mathscr{B}_j| \ll \frac{x(\log_2 x)^{j-1}T_{j-1}}{d\log x}\left(\sum_{\log_3 \phi(n_3)\leqslant M/10}\frac{1}{\phi(n_3)} + \sum_{\log_3 y > M/10}\frac{B_j(y)}{y^2}\right). \tag{5.21}$$

If M_2 is large enough, then

$$\sum_{\log_3 \phi(n_3)\leqslant M/10}\frac{1}{\phi(n_3)} \leqslant \left(\sum_{\log_2 p \leqslant e^{M/10}+1}\frac{1}{p-1}\right)^{L-j+1} \leqslant e^{(L-j+1)M/9}. \tag{5.22}$$

We will show below that

$$B_j(y) \ll \frac{y}{\log y(\log_2 y)^2} \qquad (\log_3 y \geqslant M/10, 0 \leqslant j \leqslant L). \tag{5.23}$$

In particular, $|\mathscr{B}_0| = B_0(x/d) \ll x/(d\log x)$. Combining (5.23) with (5.10), (5.21), Corollary 3.5 and (5.22), we obtain for $j \geqslant 1$,

$$\begin{aligned}|\mathscr{B}_j| &\ll \frac{x}{d\log x}(\log_2 x)^{j-1}T_{j-1}\exp\{(L-j+1)M/9\}\\ &\ll \frac{x}{d\log x}(\log_2 x)^{L}T_{L}\exp\{(L-j+1)(M/9 - M/2C - (L-j+1)/4C)\}.\end{aligned}$$

Summing over j and using Corollary 3.5, (4.1), (5.17) and (5.19) gives

$$V_\kappa(x) \geqslant \frac{|\mathscr{B}|}{2} \gg_\varepsilon d^{-1-\varepsilon}V(x).$$

This completes the proof of Theorem 2. The lower bound in Theorem 1 follows by taking $d = 1$, $\kappa = 2$.

We now prove (5.23). For $j \leqslant L-2$, $p_j \leqslant y$, hence by (5.14),

$$\left(\frac{\log_2 p_{j+1}}{\log_2 y}, \cdots, \frac{\log_2 p_L}{\log_2 y}\right) \in \mathscr{S}_{L-j}((\xi_j, \ldots, \xi_{L-1})). \tag{5.24}$$

Thus, by Lemma 3.8 and (5.16) (and trivially when $j \geqslant L-1$),

$$1 \leqslant \log_2 p_L \leqslant 3\varrho^{L-j}\log_2 y,$$

which implies

$$h := \omega(n_3) = L-j+1 \leqslant 2C\log_3 y + 3. \tag{5.25}$$

Next define

$$S = \exp\exp\{(\log_3 y)^{10}\}. \tag{5.26}$$

We remove from consideration those n_3 satisfying (i) $n_3 \leqslant y/\log^2 y$, (ii) $p^2|\phi(n_3)$ for some prime $p > \log^2 y$, (iii) there is some $m|n_3$ with $m > \exp((\log_2 y)^2)$ and $P^+(m) < m^{1/\log_2 y}$; (iv) n_3 is divisible by a prime which is not S-normal. If $p^2|\phi(n_3)$, then either $p^2|n_3$ or n_3 is divisible by two primes $\equiv 1 \pmod p$. Thus, the number of n_3 satisfying (ii) is

$$\leqslant \sum_{p>\log^2 y}\left[\frac{y}{p^2} + y\left(\sum_{q<y, q\equiv 1 \pmod p}\frac{1}{q}\right)^2\right] \ll \sum_{p>\log^2 y}\frac{y(\log_2 y)^2}{p^2} \ll \frac{y(\log_2 y)^2}{\log^2 y}$$

by the Brun-Titchmarsh inequality and partial summation. By Lemma 2.3, the number of n_3 satisfying (iii) is $O(y/\log^2 y)$. By the Hardy-Ramanujan inequality [22], the number of integers $\leqslant t$ which have $h-1$

prime factors is $O(t(\log_2 t + O(1))^{h-2}/((h-2)!\log t))$ uniformly for $h \geqslant 2$. Thus, the number of n_3 satisfying (iv) is

$$\ll \sum_{\substack{p\leqslant y \\ p \text{ not } S-\text{normal}}} \frac{y\exp(2(\log_3 y)^2)}{p\log(2y/p)} \ll \frac{y}{(\log y)(\log_2 y)^2}$$

by Lemma 2.6 and partial summation (if $j = L$, then $h = 1$ and we use Lemma 2.6 directly).

For the remaining n_3, since $\log_3 y \geqslant M/10$, by (5.10) we have

$$\log d \leqslant (10\log_3 y)^9. \tag{5.27}$$

Let n_4 be the unique number associated with n_3. As $\phi(n_4) \leqslant dy$, we have $n_4 \ll y(\log y)^{1/3}$. Now remove from consideration those n_3 with (v) $p^2|n_4$ or $p^2|\phi(n_4)$ for some prime $p > \log^2 y$. The number of such n_3 is $O(y/\log^{3/2} y)$. Also remove from consideration those n_3 such that (vi) n_4 is divisible by a prime which is not S-normal. By the way we chose n_4, the only way this is possible is if d_1 has a prime factor which is not S-normal, or if $\phi(n_3) \neq \phi(n_3')$ for $n_3' \in \mathscr{A}_j$, $n_3' \neq n_3$. The first case is not possible, since by (5.27), $d_1 \ll d\log_2 d \ll \log S$, hence for $p|d_1$, $\Omega(p-1) \leqslant 2\log p \leqslant 2\log d_1 \leqslant \log_2 S + O(1)$. For n_3 in the latter category, the numbers $\phi(n_4)$ are distinct totients. Hence, by Lemma 2.8 and (4.1), the number of such n_3 is

$$\ll \frac{y(\log_2 y)^6 W(y)}{\log y}(\log S)^{-1/6} \ll \frac{y}{\log y(\log_2 y)^2}.$$

Let $B_j^*(y)$ denote the number of remaining n_3 (those not satisfying any of conditions (i)–(vi) above), so that

$$B_j(y) \ll \frac{y}{\log y(\log_2 y)^2} + B_j^*(y). \tag{5.28}$$

If $j \leqslant L-1$, then $p_{j+1}\cdots p_L \leqslant p_{j+1}^h$, so by (5.10), (5.15), (5.25), and $M \leqslant 10\log_3 y$,

$$\log_2(n_3/p_j) \leqslant \frac{\log_2 p_j}{1+\frac{1}{10}(h+M-1)^{-3}} + \log h \leqslant \log_2 y - 2\log_3 y \leqslant \log_2 y - 10.$$

In particular, since $n_3 > y/\log^2 y$, this shows that

$$p_j > y^{9/10}, \qquad p_{j+1} < y^{1/(100\log_2 y)}. \tag{5.29}$$

When $j = L$, the first inequality in (5.29) holds since $n_3 > y/\log^2 y$, and the second inequality is vacuous. Note that p is $S-$normal for all $p|n_3n_4$, and hence by (2.2),

$$P^+(p-1) \geqslant (p-1)^{1/\Omega(p-1)} \geqslant p^{1/(4\log_2 y)}. \tag{5.30}$$

We now group the n_3 counted in $B_j^*(y)$ according to the sizes of $P^+(p_i-1)$. Let J be the largest index with $\log_2 P^+(p_J-1) > (\log_2 y)^{2/3}$. By (5.29), $J \geqslant j$. Set $\varepsilon = 1/\log_2 y$. For each n_3, there are numbers $\zeta_{j+1},\ldots,\zeta_J$, each an integral multiple of ε, and with $\zeta_i - \varepsilon \leqslant \frac{\log_2 P^+(p_i-1)}{\log_2 y} \leqslant \zeta_i$ for each i. Also set $\zeta_j = 1$ and

$$\zeta_{J+1} = \min\left(\frac{\zeta_J}{1+\omega_J} + \frac{\log_3 y + \log 4}{\log_2 y}, (\log_2 y)^{-1/3}\right). \tag{5.31}$$

By (5.30),

$$\log_2 P^+(p_i-1) \leqslant \zeta_{J+1} \qquad (i > J). \tag{5.32}$$

By (5.14) and (5.25),

$$\sum_{i=1}^{J-j} a_i\zeta_{j+i} \leqslant 1 - \omega_j + h^2\varepsilon \leqslant 1 - \omega_j/2. \tag{5.33}$$

Let $\delta = \sqrt{\log_2 S/\log_2 y}$. We claim that

$$\left| \frac{\log_2 P^+(p_i-1) - \log_2 P^+(q_i-1)}{\log_2 y} \right| \leqslant (2(i-j)+1)\delta \qquad (j \leqslant i \leqslant J). \tag{5.34}$$

To see this, fix i, let $k = i-j$ and

$$\alpha = \frac{\log_2 P^+(p_i-1)}{\log_2 y}, \qquad \beta = \frac{\log_2 P^+(q_i-1)}{\log_2 y}.$$

By (2.2), if $\beta > \alpha + (2k+1)\delta$, then

$$(k+1)(\beta-\alpha-\delta) \leqslant \frac{\Omega(\phi(n_3), P^+(p_i-1), P^+(q_i-1)}{\log_2 y} \leqslant k(\beta-\alpha+\delta),$$

a contradiction. Assuming $\beta < \alpha - (2k+1)\delta$ likewise leads to a contradiction. This establishes (5.34). In particular, (5.34) implies that $q_{j+1}, \ldots, q_J$ exist.

By (5.15), (5.25), (5.30) and $\log_3 y \geqslant M/10$, for $j \leqslant i \leqslant J$,

$$\begin{aligned} \zeta_i &\geqslant \frac{\log_2 p_i - \log_3 y - \log 4}{\log_2 y} \geqslant (1+\omega_i)(\zeta_{i+1}-\varepsilon) - \frac{\log_3 y + \log 4}{\log_2 y} \\ &\geqslant \zeta_{i+1} + \frac{(\log_2 y)^{-1/3}}{10(M+h)^3} - 2\varepsilon \log_3 y \geqslant \zeta_{i+1} + (\log_2 y)^{-0.35}. \end{aligned} \tag{5.35}$$

We make a further subdivision of the numbers n_3, counting separately those with $(p_j \cdots p_J, q_j \cdots q_J) = m$. Let $B_j(\boldsymbol{\zeta}; m; y)$ be the number of n_3 counted by $B_j^*(y)$ satisfying

$$y^{9/10} \leqslant p_j \leqslant y, \quad \zeta_i - \varepsilon \leqslant \frac{\log_2 P^+(p_i-1)}{\log_2 y} < \zeta_i \qquad (j+1 \leqslant i \leqslant J).$$

Fix $m, \boldsymbol{\zeta}$ and suppose n_3 is counted in $B_j(\boldsymbol{\zeta}; m; y)$. Let $p_j \cdots p_J/m = p_{j_0} \cdots p_{j_{k-1}}$, where

$$j = j_0 < j_1 < \cdots < j_{k-1} \leqslant J.$$

Let $\nu_0 = 1$, for $1 \leqslant i \leqslant k-1$ let $\nu_i = \zeta_{j_i} + (2L+1)\delta$, and for $0 \leqslant i \leqslant k-1$ let $\mu_i = \nu_i - (4L+2)\delta - \varepsilon$. Also, put $\nu_k = \zeta_{J+1} + (2L+3)\delta$. For brevity, for $0 \leqslant i \leqslant k-1$ set $u_i = \exp[(\log y)^{\mu_i}]$ and for $0 \leqslant i \leqslant k$ set $v_i = \exp[(\log y)^{\nu_i}]$. By (5.32), $P^+(p_i-1) \leqslant v_k$ for $i > J$. We also claim that $P^+(q_i-1) \leqslant v_k$ for $i < J$. If not, then by the $S-$normality of the primes p_i and q_i,

$$(J-j+2)(\nu_k - \zeta_{J+1} + \delta \log_2 y) \leqslant \Omega(\phi(n_3), \exp[(\log y)^{\zeta_{J+1}})], v_k) \leqslant (J-j+1)(\nu_k - \zeta_{J+1} + \delta \log_2 y),$$

a contradiction. Hence, $B_j(\boldsymbol{\zeta}; m; y)$ is at most the number of solutions of

$$(p_{j_0}-1) \cdots (p_{j_{k-1}}-1)(p_{J+1}-1) \cdots (p_L-1)d = (q_{j_0}-1) \cdots (q_{j_{k-1}}-1)e \leqslant y/\phi(m), \tag{5.36}$$

where $P^+((p_{J+1}-1) \cdots (p_L-1)e) \leqslant v_k$, and p_{j_i} and q_{j_i} are S-normal primes satisfying

$$u_i \leqslant P^+(p_{j_i}-1), P^+(q_{j_i}-1) \leqslant v_i \qquad (0 \leqslant i \leqslant k-1). \tag{5.37}$$

By (5.29), $\phi(m) \leqslant y^{1/10}$. Also, $p_j - 1$ cannot be divisible by a factor $b > y^{1/3}$ with $P^+(b) < y^{1/9 \log_2 y}$. Further, (5.35) and the definition of ν_k imply that $\nu_{i-1} - \nu_i \geqslant 2\delta$ for $2 \leqslant i \leqslant k$. By Lemma 5.1,

$$B_j(\boldsymbol{\zeta}; m; y) \ll \frac{y}{d\phi(m)} (c_4 \log_2 y)^{6L+6} (L+2)^{\Omega(d)} (\log v_k)^{20(L+1)^2} (\log y)^{-2+\sum_{i=1}^{k-1} a_i \zeta_{j_i} + E},$$

where $E \ll \delta L^2 \log L$. By (5.33), the exponent of $\log y$ is at most $-1 - \omega_j/2 + E$. By (5.27), $\Omega(d) \ll \log d \ll (\log_3 y)^9$, hence

$$B_j(\boldsymbol{\zeta}; m; y) \ll \frac{y}{d\phi(m)} (\log y)^{-1-\omega_j/2} \exp\{O((\log_2 y)^{2/3} (\log_3 y)^2)\}.$$

Also,

$$\sum_m \frac{1}{\phi(m)} \leqslant (\log_2 y + O(1))^{L-j} \ll \exp\{O((\log_3 y)^2)\}.$$

The number of possibilities for $\boldsymbol{\zeta}$ is at most $\varepsilon^{-L} \leqslant \exp\{2(\log_3 y)^2\}$. Summing over all possible m and $\boldsymbol{\zeta}$, and applying $\log_3 y \geqslant M/10$, we have

$$\begin{aligned} B_j^*(y) = \sum_{\boldsymbol{\zeta},m} B_j(\boldsymbol{\zeta}; m; y) &\ll \frac{y}{\log y}(\log y)^{-\omega_j/2+(\log_2 y)^{-1/4}} \\ &\ll \frac{y}{\log y} \exp\left\{ \frac{-\log_2 y}{20(2C\log_3 y + M + 3)^3} + (\log_2 y)^{3/4} \right\} \\ &\ll \frac{y}{\log y} \exp\{-(\log_2 y)^{9/10}\}. \end{aligned}$$

Combining this with (5.28) completes the proof of (5.23).

6 The normal multiplicative structure of totients

The proofs of Theorems 1 and 2 suggest that for most totients $m \leqslant x$, all the pre-images n of m satisfy $(x_1, x_2, \ldots, x_L) \in S_L(\boldsymbol{\xi})$ with L near L_0 and $\boldsymbol{\xi}$ defined as in section 4. We prove such a result below in Theorem 16, which is an easy consequence of Theorem 1 and the machinery created for its proof. From this, we deduce the normal size of the numbers $q_i(n)$ and establish Theorems 10 and 11. Using these bounds, we deduce the normal order of $\Omega(m)$ (Theorem 12 and Corollary 13).

Theorem 16. *Suppose* $0 \leqslant \Psi < L_0(x)$, $L = L_0 - \Psi$ *and let*

$$\xi_i = \xi_i(x) = 1 + \frac{1}{10000} e^{-(L_0-i)/40} \qquad (0 \leqslant i \leqslant L-1). \tag{6.1}$$

The number of totients $m \leqslant x$ *with a pre-image* n *satisfying*

$$(x_1(n;x), \ldots, x_L(n;x)) \notin \mathscr{S}_L(\boldsymbol{\xi}) \quad \textit{or} \quad x_L(n;x) \leqslant \frac{2}{\log_2 x} \tag{6.2}$$

is $\ll V(x)\exp\{-\Psi^2/4\}$.

Proof. As in Section 4, define $M_j(x)$ to be the number of totients $m \leqslant x$ with a pre-image satisfying (I_i) for $i < j$, but not satisfying (I_j), where $\mathbf{x} = (x_1(n;x), \ldots, x_L(n;x))$. By Theorem 1, Corollary 3.5, and (4.8), the number of totients $m \leqslant x$ with a pre-image n satisfying $\mathbf{x} \notin \mathscr{S}_L(\boldsymbol{\xi})$ is at most

$$\sum_{j \leqslant L-1} M_j(x) \ll \frac{x}{\log x} Z(x) e^{-\Psi^2/4} \ll V(x) e^{-\Psi^2/4}.$$

Now suppose that $\mathbf{x} \in \mathscr{S}_L(\boldsymbol{\xi})$ and $x_L \leqslant 2/\log_2 x$. Then $q_L(n) \leqslant e^{e^2}$. We can assume that $x/\log x \leqslant n \leqslant 2x\log_2 x$ and that n is S-nice, where $S = \exp\{(\log_2 x)^{100}\}$, the number of exceptions being $\ll V(x)/\log_2 x$. By Lemma 2.2, we can also assume that $\Omega(n) \leqslant 10\log_2 x$. Put $p_i := q_i(n)$. Lemma 3.8 gives $x_3 < 5\varrho^3 < 0.9$, and so $p_2 \leqslant \exp((\log x)^{0.9})$. Thus,

$$n/(p_0p_1p_2) = p_3p_4\cdots \leqslant \exp(10(\log_2 x)(\log x)^{0.9}) \ll x^{1/100}$$

and so $p_0 \geqslant x^{1/4}$ for large x. In particular, $p_0^2 \nmid n$.

Suppose now that n has exactly $L_0 - k + 1$ prime factors $> e^{e^2}$, where we fix $k > \Psi$. Then

$$v = (p_0 - 1)\phi(p_1p_2\cdots p_{L_0-k})w$$

for some integer w satisfying $P^+(w) \leqslant e^{e^2}$. Using the prime number theorem to estimate the number of choices for p_0 given $p_1 \cdots p_{L_0-k}$ and w, we obtain that the number of v of this form is

$$\ll \frac{x}{\log x} \sum_{p_1,\ldots,p_{L_0-k}} \frac{1}{\phi(p_1 \cdots p_{L_0-k})} \sum_w \frac{1}{w} \ll \frac{x}{\log x} R_{L_0-k}(\boldsymbol{\xi}_k; x),$$

since $p_1 \cdots p_{L_0-k} \in \mathscr{R}_{L_0-k}(\boldsymbol{\xi}_k; x)$, where $\boldsymbol{\xi}_k := (\xi_0, \ldots, \xi_{L_0-k-1})$. By Lemma 3.1, Corollary 3.5, and Lemma 3.10 (ii),

$$R_{L_0-k}(\boldsymbol{\xi}_k; x) \ll (\log_2 x)^{L_0-k} T_{L_0-k} \ll Z(x) \exp(-k^2/4C),$$

hence the number of totients is

$$\ll \frac{x}{\log x} Z(x) \exp(-k^2/4C) \ll V(x) \exp(-k^2/4C).$$

Summing over $k > \Psi$ gives the required bound. □

We show below that for most of $\mathscr{S}_L$, $x_j \approx \varrho^j(1-j/L)$ for $1 \leqslant j \leqslant L$. Let $T_L^*(\mathscr{R}) = \mathrm{Vol}\,(\mathscr{S}_L^* : \mathscr{R})$, recall definition (3.3) and Lemma 3.7. Define

$$\lambda_i = \varrho^i g_i \quad (i \geqslant 0), \qquad \lambda = \lim_{i\to\infty} \lambda_i = \frac{1}{\varrho F'(\varrho)} < \frac{1}{3}. \tag{6.3}$$

By Lemma 3.7 and explicit calculation of g_i for small i, we have for large L

$$\frac{1}{5} \leqslant \lambda_i \leqslant \frac{1}{3}, \qquad , \frac{g_i g_{L-i}}{g_L} \leqslant \frac{1}{3}, \qquad \frac{g_i g_{L-i}^*}{g_L^*} \leqslant \frac{1}{3}. \tag{6.4}$$

Lemma 6.1. *Suppose $i \leqslant L-2$, $\beta > 0$, $\alpha \geqslant 0$ and define θ by*

$$\beta = \frac{\varrho^i(1-i/L)}{1+\theta}. \tag{6.5}$$

If $\theta > 0$, then

$$T_L^*(x_i \leqslant \beta, x_L \geqslant \alpha) \ll T_L \frac{i}{\theta L} \frac{(1+\theta L/i)^i}{(1+\theta)^L} e^{-L\alpha g_L}. \tag{6.6}$$

For $-\lambda_i \leqslant \theta \leqslant 0$,

$$T_L^*(x_i \geqslant \beta, x_L \geqslant \alpha) \ll T_L e^{-\frac{2}{3}L\alpha g_L} \exp\left\{ Ki + \frac{\lambda_i}{1-\lambda_i} L\theta + L(\theta - \log(1+\theta)) \right\}, \tag{6.7}$$

where $K = \frac{\lambda}{1-\lambda} + \log(1-\lambda) = 0.0873\ldots$. If $-i\lambda_i/L < \theta < 0$, then

$$T_L^*(x_i \geqslant \beta, x_L \geqslant \alpha) \ll T_L e^{-\frac{2}{3}L\alpha g_L} \frac{i}{|\theta| L} \exp\left\{ -\frac{L(L-i)}{2i} \theta^2 \right\}. \tag{6.8}$$

Proof. For each inequality, we show that the region in question lies inside a simplex for which we may apply Lemma 3.6. The volume is then related to T_L via Lemma 3.4. By Lemma 3.8, $x_L \leqslant 1/g_L$. Hence, we may assumer $\alpha \geqslant 1/g_L$, else the volumes are all zero. Also by Lemma 3.8, $x_i \geqslant \alpha g_{L-i}$, so we may assume that $\beta > \alpha g_{L-i}$ in showing (6.6). Also, if $\beta \leqslant \alpha g_{L-i}$, then $T_L^*(x_i \geqslant \beta, x_L \geqslant \alpha) = T_L(x_L \geqslant \alpha)$ (i.e., doesn't depend on β), while the right sides of (6.7) and (6.8) are each increasing in θ. Thus, for (6.7) and (6.8), we may assume also that $\beta > \alpha g_{L-i}$ as well.

All three inequalities are proved by a common method. Consider $\mathbf{x} \in \mathscr{S}_L$ with $x_L \geqslant \alpha$ and let $y_j = x_j - \alpha g_{L-j}$ for each j. Then $\mathbf{v}_j \cdot \mathbf{y} = \mathbf{v}_j \cdot \mathbf{x} \leqslant 0$ $(1 \leqslant j \leqslant L)$ and $\mathbf{v}_0 \cdot \mathbf{y} \leqslant 1 - \alpha g_L$. Let $\xi = 1 - \alpha g_L$ and $\beta' = \beta - \alpha g_{L-i}$. Set $z_j = y_j - \beta' g_{i-j}$ for $j \leqslant i$ and $z_j = y_j$ for $j > i$. By (3.3),

$$\begin{aligned} &\mathbf{v}_j \cdot \mathbf{z} \leqslant 0 \qquad (1 \leqslant j \leqslant L, j \neq i), \\ &\mathbf{v}_i \cdot \mathbf{z} \leqslant \beta', \\ &\mathbf{v}_0 \cdot \mathbf{z} \leqslant \xi - \beta' g_i. \end{aligned} \tag{6.9}$$

With these definitions, $x_i \lesseqgtr \beta \iff z_i \lesseqgtr 0$. Hence, for any $A \geqslant -g_i$, we have

$$\begin{aligned} &\mathbf{v}_0' \cdot \mathbf{z} \leqslant \xi + A\beta', \quad \mathbf{v}_0' = (\mathbf{v}_0 + (g_i + A)\mathbf{v}_i), \\ &\mathbf{v}_j \cdot \mathbf{z} \leqslant 0 \quad (1 \leqslant j \leqslant L, j \neq i), \\ \pm &\mathbf{e}_i \cdot \mathbf{z} \leqslant 0. \end{aligned} \tag{6.10}$$

In the last inequality, we take $+$ for (6.7) and (6.8), and $-$ for (6.6). By (3.3), (3.7) and (3.8),

$$\mathbf{v}_0' + \sum_{j<i} g_j \mathbf{v}_j + A\mathbf{e}_i + \sum_{j=i+1}^{L-1} (g_j + Ag_{j-i})\mathbf{v}_j + (g_L^* + Ag_{L-i}^*)\mathbf{v}_L = \mathbf{0}. \tag{6.11}$$

To ensure that each vector on the left of (6.10) has a positive coefficient, we assume that $A > 0$ for proving (6.6), and $A < 0$ otherwise. We may also assume that $\xi - \beta' g_i > 0$, else the volume in question is zero by (6.9) (each coordinate of $\mathbf{z}$ is non-negative). By Lemma 3.6, together with (3.9), Lemma 3.7 and (6.4),

$$\begin{aligned} T_L(x_i \lesseqgtr \beta, x_L \geqslant \alpha) &\leqslant T_L^* \frac{g_i}{|A|}(\xi + A\beta')^L \prod_{j=i+1}^{L-1} \left(1 + A\frac{g_{j-i}}{g_j}\right)^{-1} \left(1 + A\frac{g_{L-i}^*}{g_L^*}\right)^{-1} \\ &\ll T_L \frac{g_i}{|A|} \frac{(\xi + A\beta')^L}{(1 + A\varrho^i)^{L-i}}. \end{aligned} \tag{6.12}$$

Since $\beta \leqslant \alpha g_{L-i} \leqslant g_{L-i}/g_L$, if $A > 0$ then

$$\xi + A\beta' = (1 + A\beta)\left(1 - \alpha g_L \frac{1 + Ag_{L-i}/g_L}{1 + A\beta}\right) \leqslant (1 + A\beta)(1 - \alpha g_L) \leqslant (1 + A\beta)e^{-\alpha g_L}.$$

Taking $A = \frac{L\theta}{i\varrho^i}$ gives (6.6). If $-g_i \leqslant A < 0$, then by (6.4),

$$\xi + A\beta' \leqslant (1 + A\beta)\left(1 - \alpha g_L(1 - g_i g_{L-i}/g_L)\right) \leqslant (1 + A\beta)e^{-\frac{2}{3}\alpha g_L}.$$

For (6.7), we take $A = -g_i$, then use

$$(1 - \lambda_i)^{i-L}(1 - \beta g_i)^L = \frac{(1 - \lambda_i)^i}{(1 + \theta)^L}\left(1 + \frac{\theta + i\lambda_i/L}{1 - \lambda_i}\right)^L \leqslant \frac{(1 - \lambda)^i}{(1 + \theta)^L} \exp\left\{\frac{\theta L + i\lambda_i}{1 - \lambda_i}\right\}$$

together with $\frac{i\lambda_i}{1-\lambda_i} = \frac{i\lambda}{1-\lambda} + O(1)$ (a corollary of Lemma 3.7). Taking $A = \frac{L\theta}{i\varrho^i}$ gives (6.8), since

$$\frac{(1 + \theta L/i)^i}{(1 + \theta)^L} = \exp\left\{\frac{L(L-i)}{i}\theta^2 \left(-\frac{1}{2} - \sum_{j=1}^{\infty} (-\theta)^j \frac{L^j + iL^{j-1} + \cdots + i^j}{(j+2)i^j}\right)\right\} \tag{6.13}$$

and all summands in the sum on j are positive. □

We apply Lemma 6.1 to determine the size of $q_i(n)$ when n is a pre-image of a "normal" totient. Recall that $V(x; \mathscr{C})$ is the number of totients $m \leqslant x$ with a pre-image n satisfying $\mathscr{C}$. An inequality we will use is

$$\sum_{\substack{v \in \mathscr{V} \\ P^+(v) \leqslant y}} \frac{1}{v} \ll e^{C(\log_3 y)^2}, \tag{6.14}$$

coming from the first part of Lemma 4.3 and Theorem 1.

Lemma 6.2. *Suppose x is large, $\beta > 0$, and $1 \leqslant i \leqslant L_0 = L_0(x)$. Define θ by $(1 + \theta)\beta = \varrho^i(1 - i/L_0)$.*

(a) If $0 < \theta \leqslant \frac{i}{3L_0}$, then $V\left(x; \frac{\log_2 q_i(n)}{\log_2 x} \leqslant \beta\right) \ll V(x)\frac{i}{\theta L_0} \exp\left\{-\frac{L_0(L_0 - i)}{4i}\theta^2\right\}$.

(b) If $\frac{i}{3L_0} \leqslant \theta \leqslant \frac{1}{8}$, then $V\left(x; \frac{\log_2 q_i(n)}{\log_2 x} \leqslant \beta\right) \ll V(x)e^{-\theta L_0/13}$.

(c) If $-\frac{1}{3} \leqslant \theta < -0.29\frac{i}{L_0}$*, then* $V\left(x; \frac{\log_2 q_i(n)}{\log_2 x} \geqslant \beta\right) \ll V(x)e^{\theta L_0/10}$.

(d) If $-\frac{i\lambda_i}{L_0} \leqslant \theta < 0$*, then* $V\left(x; \frac{\log_2 q_i(n)}{\log_2 x} \geqslant \beta\right) \ll V(x)\frac{i}{|\theta| L_0} \exp\left\{-0.49\frac{L_0(L_0-i)}{i}\theta^2\right\}$.

Proof. Let A be a sufficiently large, absolute constant. We may assume that

$$A \leqslant i \leqslant L_0 - A,\ |\theta| \geqslant A\left(\frac{i}{L_0(L_0-i)}\right)^{1/2} \qquad \text{for (a) and (d),}$$
$$|\theta| \geqslant \frac{A}{L_0} \qquad \text{for (b) and (c),} \tag{6.15}$$

for otherwise the claims are trivial. Put $\Psi = \left\lceil |\theta|\sqrt{\frac{2L_0(L_0-i)}{i}}\right\rceil$ for (a) and (d), and put $\Psi = \left\lceil \sqrt{2|\theta| L_0}\right\rceil$ for parts (b) and (c). Let $L = L_0 - \Psi$. By (6.15), for the range of θ given in each part, we have $i \leqslant L-2$. Define ξ_i by (6.1). By Theorem 16, the number of totients $m \leqslant x$ with a preimage n satisfying $\mathbf{x} \notin \mathscr{S}_L(\boldsymbol{\xi})$, $x_L \leqslant \frac{2}{\log_2 x}$ or $m < \frac{x}{\log x}$ is $O(V(x)e^{-\frac14\Psi^2})$. Let $\mathscr{S} = \mathscr{S}_L(\boldsymbol{\xi}) \cap \{x_i \leqslant \beta\}$ for (a) and (b), and $\mathscr{S} = \mathscr{S}_L(\boldsymbol{\xi}) \cap \{x_i \geqslant \beta\}$ for (c) and (d). As in the proof of (4.10), for $b \geqslant 2$ let $N_b(x)$ be the number of totients for which $n > \frac{x}{\log x}$, $\mathbf{x} \in \mathscr{S}$, and $\frac{b}{\log_2 x} \leqslant x_L < \frac{b+1}{\log_2 x}$. By the argument leading to (4.10) and using (6.14),

$$V\left(x; \frac{\log_2 q_i(n)}{\log_2 x} \lesseqgtr \beta\right) \ll V(x)e^{-\Psi^2/4} + \frac{x}{\log x}\sum_{b\geqslant 2} e^{C\log^2 b} R_L\left(\mathscr{S} \cap \left\{x_L \geqslant \frac{b}{\log_2 x}\right\}; x\right). \tag{6.16}$$

By Lemma 3.1,

$$R_L\left(\mathscr{S} \cap \left\{x_L \geqslant \frac{b}{\log_2 x}\right\}; x\right) \ll (\log_2 x)^L \operatorname{Vol}\left[\mathscr{S} \cap \{x_L \geqslant b/\log_2 x\}\right]^{+\varepsilon}, \quad \varepsilon = \frac{1}{\log_2 x}.$$

Let $\alpha = \frac{b}{\log_2 x}$. By Lemma 3.9 ($\alpha'$, y_j and ξ_j' defined here), $\mathbf{y} \in \mathscr{S}_L^*$, $y_i \lesseqgtr \beta'$ and $y_L \geqslant \alpha'$, where

$$\beta' = \frac{\beta}{\xi_0' \cdots \xi_{i-1}'} = \beta\left(1 - O\left(e^{-(L_0-i)/40}\right)\right). \tag{6.17}$$

By Lemma 3.2 and Corollary 3.3,

$$\operatorname{Vol}\left[\mathscr{S} \cap \{x_L \geqslant b/\log_2 x\}\right]^{+\varepsilon} \ll T_L^*\left(x_i \lesseqgtr \beta', x_L \geqslant \alpha'\right). \tag{6.18}$$

Define θ' by $1+\theta' = (1+\theta)\xi_0'\cdots\xi_{i-1}'$, so that $\beta'(1+\theta') = \varrho^i(1-i/L)$. By (6.17), $\theta' - \theta = (1+\theta)(\xi_0'\cdots\xi_{i-1}' - 1) \ll e^{-\frac{1}{40}(L_0-i)}$. By (6.15), if A is large enough then

$$0 < \theta' - \theta \leqslant Ae^{-\frac{1}{40}(L_0-i)} \leqslant \frac{|\theta|}{1000}. \tag{6.19}$$

We now apply Lemma 6.1 (with β, θ replaced by β', θ'). For parts (a) and (b), (6.19) implies $0 < \theta' \leqslant \frac17$ and we may apply (6.6). For (c), (6.19) implies $-\frac18 \leqslant \theta' \leqslant -0.288\frac{i}{L_0}$ and we apply (6.7). For (d), (6.19) gives $-\frac{i\lambda_i}{L_0} \leqslant \theta' < 0$ and we apply (6.8). Combining these estimates with (6.18), we arrive at

$$R_L\left(\mathscr{S} \cap \left\{x_L \geqslant \frac{b}{\log_2 x}\right\}; x\right) \ll (\log_2 x)^L T_L B e^{-\frac23 \alpha' g_L}, \tag{6.20}$$

where

$$B = \begin{cases} \frac{i}{\theta' L}\frac{(1+\theta' L/i)^i}{(1+\theta')^L} & \text{for (a),(b)} \\ \exp\left\{Ki + \frac{\lambda_i}{1-\lambda_i}\theta' L + L(\theta' - \log(1+\theta'))\right\} & \text{for (c)} \\ \frac{i}{(-L\theta')}\exp\left\{-\frac{L(L-i)}{2i}(\theta')^2\right\} & \text{for (d).} \end{cases}$$

By (1.7) and Lemma 3.7, we have $\alpha' L g_L \gg \alpha L \varrho^{-L} \gg \varrho^{-\Psi}$. Hence, for some absolute constant $C_1 > 0$,

$$\sum_{b\geqslant 2} e^{C\log^2 b - \frac{2}{3}\alpha' L g_L} \ll \varrho^{-\Psi} \sum_{k\geqslant 0} e^{C\log^2((k+1)\varrho^{-\Psi}) - C_1 k} = \exp\left\{ \frac{\Psi^2}{4C} + O(\Psi) \right\}.$$

Since Corollary 3.5 implies that $(\log_2 x)^L T_L \ll Z(x)\exp\{-\Psi^2/(4C) + O(\Psi)\}$, inequalities (6.16) and (6.20) now imply

$$V\left(x; \frac{\log_2 q_i(n)}{\log_2 x} \lesseqgtr \beta\right) \ll V(x)\left[e^{-\frac{1}{4}\Psi^2} + Be^{O(\Psi)} \right].$$

To complete part (a), observe that the absolute value of the summands in (6.13) (with θ replaced by θ') are decreasing. From the definition of Ψ and (6.19), we obtain $O(\Psi) \leqslant \frac{L_0(L_0-i)}{100i}\theta^2 + O(1)$ and

$$\begin{aligned} B &\leqslant \exp\left\{ \frac{L(L-i)}{i}(\theta')^2 \left(-\frac{1}{2} + \frac{L+i}{3i}\theta' \right) \right\} \leqslant \exp\left\{ -\frac{5(\theta')^2 L(L-i)}{18i} \right\} \\ &\leqslant \exp\left\{ -0.27\frac{L(L-i)}{i}\theta^2 \right\} \ll \exp\left\{ -0.26\frac{L_0(L_0-i)}{i}\theta^2 \right\}. \end{aligned}$$

this gives part (a) of the lemma. For (b), (6.19) implies $\theta' L/i \geqslant 0.33$, so $i\log(1+\theta' L/i) \leqslant 0.08642 L\theta'$. Also, $\log(1+\theta') \geqslant 0.9423\theta'$. Therefore, $B \leqslant e^{-0.0781 L\theta'} \ll e^{-0.077 L_0\theta}$, whence $Be^{O(\Psi)} \ll e^{-\frac{1}{13}L_0\theta}$. For (c), we use $\theta' - \log(1+\theta') \leqslant 0.0683\theta'$. If $i \leqslant 100$, $Ki = O(1)$ and $\frac{\lambda_i}{1-\lambda_i} \geqslant \frac{\lambda_1}{1-\lambda_1} \geqslant 0.265$, and for $i > 100$, $Ki \leqslant 0.302(-L\theta')$ and $\frac{\lambda_i}{1-\lambda_i} \geqslant 0.4781$. In either case, $B \ll e^{0.106 L\theta'}$ and therefore $Be^{O(\Psi)} \ll e^{\frac{1}{10}L_0\theta}$ by (6.19). Finally, part (d) follows from (6.19) by similar calculations to those in part (a). □

Proof of Theorem 10. Let $x_i = \frac{\log_2 q_i(n)}{\log_2 x}$. Consider first the case $0 \leqslant \varepsilon \leqslant \frac{i}{3L_0}$. If $x_i \leqslant (1-\varepsilon)\beta_i \leqslant \frac{\beta_i}{1+\varepsilon}$, take $\theta = \varepsilon$ in Lemma 6.2 (a). If $x_i \geqslant (1+\varepsilon)\beta_i$, take $\theta = -\frac{\varepsilon}{1+\varepsilon} \in [-\varepsilon, -\frac{3}{4}\varepsilon]$. Use Lemma 6.2 (d) if $\theta \geqslant -\frac{i\lambda_i}{L_0}$ and Lemma 6.2 (c) otherwise. This yields the desired bounds, since in the latter case $\theta \geqslant -\frac{4i}{10(L_0-i)}$.

Next, assume $\frac{i}{3L_0} \leqslant \varepsilon \leqslant \frac{1}{8}$. If $x_i \leqslant (1-\varepsilon)\beta_i$, take $\theta = \varepsilon$ in Lemma 6.2 (b). If $x_i \geqslant (1+\varepsilon)\beta_i$, take $\theta = -\frac{\varepsilon}{1+\varepsilon} \in [-\varepsilon, -\frac{8}{9}\varepsilon]$ in Lemma 6.2 (c). We may do so since $\theta \leqslant -0.29\frac{i}{L_0}$. □

Proof of Theorem 11. Assume $g \geqslant 10$ and $h \geqslant 10$, for otherwise the conclusion is trivial. Let

$$\varepsilon_i = g\sqrt{\frac{i\log(L_0-i)}{L_0(L_0-i)}} \qquad (1 \leqslant i \leqslant L_0 - h)$$

and let N_i be the number of totients $\leqslant x$ with a preimage satisfying $|\frac{\log_2 q_i(n)}{\beta_i \log_2 x} - 1| \geqslant \varepsilon_i$. First, suppose that $\varepsilon_i \leqslant \frac{i}{3L_0}$, and let $k = L_0 - i$. We have $\frac{k}{\log k} \geqslant 4g^2$, for if not, then $k < 4g^2 \log L_0 < \frac{1}{2}L_0$ and consequently $\varepsilon_i > g\sqrt{\frac{\log k}{2k}} > g^2 > 10$. By Theorem 10,

$$N_i \ll V(x)\exp\left[-\frac{g^2\log(L_0-i)}{4} + \frac{1}{2}\log\left(\frac{i(L_0-i)}{g^2 L_0}\right) \right] \ll V(x)(L_0-i)^{\frac{1}{2}-\frac{1}{4}g^2}.$$

Summing over $i \leqslant L_0 - 4g^2$ and using $g \geqslant 10$, we obtain

$$\sum_{\varepsilon_i \leqslant i/(3L_0)} N_i \ll V(x)(4g^2)^{\frac{3}{2}-\frac{1}{4}g^2} \ll V(x) g^{-\frac{1}{2}g^2}. \tag{6.21}$$

Next, suppose that $\frac{i}{3L_0} < \varepsilon_i \leqslant \frac{1}{8}$. Since $i \leqslant 9g^2\frac{L_0\log(L_0-i)}{L_0-i} \leqslant 18g^2\log L_0$, Theorem 10 gives

$$\sum_{i/(3L_0) < \varepsilon_i \leqslant 1/8} N_i \ll V(x) g^2 (\log L_0) e^{-\frac{g}{13}\sqrt{\log L_0}} \ll V(x) e^{-\frac{g}{14}\sqrt{\log L_0}}. \tag{6.22}$$

Finally, if $\varepsilon_i > \max(\frac{i}{3L_0}, \frac{1}{8})$, then $|\frac{\log_2 q_i(n)}{\beta_i \log_2 x} - 1| \geqslant \varepsilon_i' := \max(\frac{i}{3L_0}, \frac{1}{8})$. By Theorem 10,

$$\begin{aligned}\sum_{\varepsilon_i > \max(i/(3L_0)),1/8)} N_i &\ll V(x)\left(L_0 e^{-\frac{1}{104}L_0} + \sum_{\frac{3}{8}L_0 < i \leqslant L_0 - h} \exp\left[-\frac{L_0(L_0-i)}{4i}\left(\frac{i}{3L_0}\right)^2 \right] \right) \\ &\ll V(x)\left(e^{-\frac{1}{105}L_0} + \sum_{i \leqslant L_0 - h} e^{-\frac{1}{96}(L_0-i)} \right) \ll V(x) e^{-\frac{h}{96}}. \end{aligned} \tag{6.23}$$

Together, inequalities (6.21)–(6.23) give Theorem 11. □

Proof of Theorem 12. Assume $\eta \geqslant \frac{1000}{\log_3 x}$, for otherwise the theorem is trivial. Let $\Psi = \Psi(x) = \lceil \sqrt{\eta \log_3 x} \rceil$, $L = L_0(x) - \Psi$, define ξ_i by (6.1) and set $S = \exp\{(\log_2 x)^{100}\}$. Let n be a generic pre-image of a totient $m \leqslant x$, and set $q_i = q_i(n)$ and $x_i = x_i(n; x)$ for $0 \leqslant i \leqslant L$. Also, define r by $m = \phi(q_0 \cdots q_L) r$. Let $\varepsilon_i = \max(0.82\eta, \frac{i}{3L_0})$. Let U be the set of totients $m \leqslant x$ satisfying one of four conditions:

(1) $(x_1, x_2, \ldots, x_L) \notin \mathscr{S}_L(\boldsymbol{\xi})$,
(2) m is not S-nice,
(3) $\exists i \leqslant \frac{L_0}{3}: \quad \left| \frac{x_i}{\beta_i} - 1 \right| \geqslant \varepsilon_i$,
(4) $\Omega(r) \geqslant (\log_2 x)^{1/2}$.

By Theorem 16 and Lemma 2.8, the number of totients $m \leqslant x$ satisfying (1) or (2) is $O(V(x)(\log_2 x)^{-\frac{1}{4}\eta})$. Theorem 10 implies that the number of totients satisfying (3) is

$$\ll V(x)\left[(\eta L_0) e^{-0.82\eta L_0/13} + \sum_{i \geqslant 2.46\eta L_0} e^{-i/39} \right] \ll V(x) e^{-\frac{1}{16}\eta L_0} \ll \frac{V(x)}{(\log_2 x)^{\eta/10}}.$$

Consider now totients satisfying (4), but neither (1), (2) nor (3). By (3), $q_1 \cdots q_L \leqslant x^{1/3}$. By Lemma 3.8,

$$\log_2 P^+(r) \leqslant x_L \log_2 x \leqslant 10\varrho^L \log_2 x \leqslant 20\varrho^{-\Psi} \log_3 x < \exp(\sqrt{\log_3 x}).$$

By Lemma 2.3, the number of totients with $r \geqslant R := \exp\exp(\frac{1}{10}\sqrt{\log_2 x})$ is $O(\frac{x}{\log x})$. Now suppose $r < R$. Given $q_1, \ldots, q_L$ and r, the number of possibilities for q_0 is

$$\ll \frac{x}{q_1 \cdots q_L r \log x}.$$

Applying Lemma 3.1, followed by Lemmas 3.4 and 3.10, gives

$$\sum \frac{1}{q_1 \cdots q_L} \leqslant R_L(\boldsymbol{\xi}) \ll Z(x) e^{-\frac{1}{4}\Psi^2} \ll Z(x)(\log_2 x)^{-\frac{1}{4}\eta}.$$

For $r \leqslant y \leqslant R$, we have $\Omega(r) \geqslant 10 \log_2 R \geqslant 10 \log_2 y$. Hence, the number of possible $r \leqslant y$ is $O(y/\log^2 y)$ by Lemma 2.2. Therefore, $\sum_r 1/r = O(1)$ and we conclude that

$$|U| \ll V(x)(\log_2 x)^{-\frac{1}{10}\eta}. \tag{6.24}$$

Assume now that a totient $m \notin U$. Since every prime factor of a preimage n is S-normal,

$$\Omega(m) = (1 + x_1 + \cdots + x_L)\log_2 x + O\left((\log_2 x)^{\frac{1}{2}} (\log_3 x)^{\frac{3}{2}} \right).$$

Since (3) fails, Lemma 3.8 implies

$$\sum_{1 \leqslant i \leqslant L} x_i \leqslant \sum_{i \leqslant L_0/3} \varrho^i (1 + 0.82\eta) + \sum_{L_0/3 < i \leqslant L} 5\varrho^{\lfloor L_0/3 \rfloor} \leqslant \frac{\varrho}{1-\varrho} + 0.98\eta$$

and

$$\sum_{1\leqslant i\leqslant L} x_i \geqslant \sum_{i\leqslant L_0/3} \beta_i(1-\varepsilon_i) \geqslant \sum_{i\leqslant L_0/3} \varrho^i(1-0.82\eta) - \sum_{i\geqslant 1} \frac{i\varrho^i}{L_0} - \sum_{i\geqslant 2.46L_0\eta} \frac{i\varrho^i}{3L_0}$$
$$\geqslant \frac{\varrho}{1-\varrho}(1-0.82\eta) - 4\varrho^{L_0/3-1} - \frac{5}{L_0} \geqslant \frac{\varrho}{1-\varrho} - 0.98\eta.$$

Therefore, if x is large then $|\Omega(m) - \frac{1}{1-\varrho}\log_2 x| \leqslant 0.99\eta\log_2 x$ for $m \notin U$. This proves the first part of Theorem 12. The second part follows easily, since a totient $m \notin U$ is S-nice and hence

$$\Omega(m) - \omega(m) \leqslant \sum_{i=0}^{L} \Omega(q_i - 1, 1, S) + \Omega(r) \ll (\log_2 x)^{1/2}. \qquad \square$$

Proof of Corollary 13. It suffices to prove the theorem with $g(m) = \Omega(m)$. Divide the totients $m \leqslant x$ into three sets, S_1, those with $\Omega(m) \geqslant 10\log_2 x$, S_2, those not in S_1 but with $|\Omega(m) - \log_2 x/(1-\varrho)| \geqslant \frac{1}{3}\log_2 x$, and S_3, those not counted in S_1 or S_2. By Lemma 2.2, $|S_1| \ll \frac{x}{\log^2 x}$ and by Theorem 12, $|S_2| \ll V(x)(\log_2 x)^{-1/30}$. Therefore

$$|S_3| = V(x)(1 - O((\log_2 x)^{-1/30})) \tag{6.25}$$

and also

$$\sum_{m\in S_1\cup S_2} \Omega(m) \ll |S_1|\log x + |S_2|\log_2 x \ll V(x)(\log_2 x)^{2/3}. \tag{6.26}$$

For each $m \in S_3$, let

$$\varepsilon_m = \frac{\Omega(m)}{\log_2 x} - \frac{1}{1-\varrho}$$

and for each integer $N \geqslant 0$, let $S_{3,N}$ denote the set of $m \in S_3$ with $N \leqslant |\varepsilon_m|\log_3 x < N+1$. By Theorem 12, (6.25) and (6.26),

$$\sum_{m\in\mathscr{V}(x)} \Omega(m) = O(V(x)\sqrt{\log_2 x}) + \sum_{0\leqslant N\leqslant \frac{1}{2}\log_3 x} \; \sum_{m\in S_{3,N}} \Omega(m)$$
$$= \frac{\log_2 x}{1-\varrho}|S_3| + O\left(V(x)\frac{\log_2 x}{\log_3 x}\sum_N (N+1)e^{-N/10}\right)$$
$$= \frac{V(x)\log_2 x}{1-\varrho}\left(1 + O\left(\frac{1}{\log_3 x}\right)\right). \qquad \square$$

7 The distribution of $A(m)$

7.1 Large values of $A(m)$

Proof of Theorem 3. First we note the trivial bound

$$|\{m \leqslant x : A(m) \geqslant N\}| \ll \frac{x\log_2 x}{N} \ll V(x)\frac{\log x}{N},$$

which implies the theorem when $N \geqslant \log^2 x$. Suppose next that $N < \log^2 x$. Suppose x is sufficiently large and set $\Psi = \lceil \log\log N \rceil$ and $L = L_0(x) - \Psi$. Note that $\Psi < \frac{3}{4}L_0(x)$. Define ξ_i by (6.1). By Theorem 16, the number of totients $m \leqslant x$ with a pre-image n satisfying $\mathbf{x}(n) \notin \mathscr{S}_L(\boldsymbol{\xi})$ is $O(V(x)e^{-\frac{1}{4}\Psi^2})$ (here $\mathbf{x}(n) = (x_1(n;x), \dots, x_L(n;x))$). For other totients m, all preimages n satisfy $\mathbf{x}(n) \in \mathscr{S}_L(\boldsymbol{\xi})$. By Lemma

3.8, $x_L = x_L(n) \leqslant 1/g_L$. For integer $b \in \{0, 1, \ldots, L-1\}$, let N_b be the number of these remaining totients $m \leqslant x$ with a preimage n satisfying

$$\frac{b}{Lg_L} \leqslant x_L < \frac{b+1}{Lg_L}.$$

Put $Y_b = \frac{b+1}{Lg_L} \log_2 x$. Write $n = q_0 \cdots q_L t$, so that $\log_2 P^+(t) \leqslant Y_b$, and let $r = \phi(t)$. Also note that $\log_2 Y_b \ll b\varrho^M$. As in the proof of (4.10), using Lemmas 3.1 and 3.10, together with (6.14) and Corollary 3.5, gives

$$\begin{aligned} N_b(x) &\ll \frac{x}{\log x} R_L(\mathscr{S}_L(\boldsymbol{\xi}) \cap \{x_L \geqslant b/(Lg_L)\}; x) \sum_r \frac{1}{r} \\ &\ll \frac{x}{\log x} e^{-C_0 b} T_L e^{C(\log Y_b)^2} \ll V(x) \exp\left\{-C_0 b + \Psi \log b + O(\Psi + \log^2 b)\right\}. \end{aligned}$$

Put $b_0 = \lceil \Psi^2/C_0 \rceil$. The number of totients with $x_L \geqslant b_0/(Lg_L)$ is therefore $\ll V(x)e^{-\Psi^2+O(\Psi \log \Psi)} \ll V(x)e^{-\frac{1}{2}\Psi^2}$. The remaining totients have all of their preimages of the form $n = q_0 \cdots q_L t$ with $\log_2 P^+(t) \leqslant Y_{b_0}$. The number of such preimages is

$$\ll \frac{x}{\log x} R_L(\mathscr{S}_L(\boldsymbol{\xi}); x) \sum_{\log_2 P^+(t) \leqslant Y_{b_0}} \frac{1}{\phi(t)} \ll V(x) e^{-C_0 b - \frac{1}{4C}\Psi^2 + Z_{b_0}}.$$

Hence, the number of totients m having at least N such preimages is

$$\ll \frac{V(x)}{N} e^{-C_0 b - \frac{1}{4C}\Psi^2 + Z_{b_0}} \ll \frac{V(x)}{N^{1/2}}.$$

□

7.2 Sierpiński's Conjecture

Schinzel's argument for deducing Sierpiński's Conjecture for a given k from Hypothesis H requires the simultaneous primality of $\gg k$ polynomials of degrees up to k. Here we preset a different approach, which is considerably simpler and requires only the simultaneous primality of three linear polynomials. We take a number m with $A(m) = k$ and construct an l with $A(lm) = k+2$. Our method is motivated by the technique used in Section 5 where many numbers with multiplicity κ are constructed from a single example.

Lemma 7.1. *Suppose $A(m) = k$ and p is a prime satisfying*

(i) $p > 2m+1$,
(ii) $2p+1$ *and* $2mp+1$ *are prime,*
(iii) $dp+1$ *is composite for all* $d|2m$ *except* $d=2$ *and* $d = 2m$.

Then $A(2mp) = k+2$.

Proof. Suppose $\phi^{-1}(m) = \{x_1, \ldots, x_k\}$ and $\phi(x) = 2mp$. Condition (i) implies $p \nmid x$, hence $p|(q-1)$ for some prime q dividing x. Since $(q-1)|2mp$, we have $q = dp+1$ for some divisor d of $2m$. We have $q > 2p$, so $q^2 \nmid x$ and $\phi(x) = (q-1)\phi(x/q)$. By conditions (ii) and (iii), either $q = 2p+1$ or $q = 2mp+1$. In the former case, $\phi(x/q) = m$, which has solutions $x = (2p+1)x_i$ $(1 \leqslant i \leqslant k)$. In the latter case, $\phi(x/q) = 1$, which has solutions $x = q$ and $x = 2q$. □

Suppose $A(m) = k$, $m \equiv 1 \pmod 3$, and let $d_1, \ldots, d_j$ be the divisors of $2m$ with $3 \leqslant d_i < 2m$. Let $p_1, \ldots, p_j$ be distinct primes satisfying $p_i > d_i$ for each i. Using the Chinese Remainder Theorem, let $a \mod b$ denote the intersection of the residue classes $-d_i^{-1} \mod p_i$ $(1 \leqslant i \leqslant j)$. For every h and i, $(a+bh)d_i + 1$ is divisible by p_i, hence composite for large enough h. The Prime k-tuples Conjecture implies that there are infinitely many numbers h so that $p = a + hb$, $2p+1$ and $2mp+1$ are simultaneously prime. By Lemma 7.1, $A(2mp) = k+2$. As $p \equiv 2 \pmod 3$, $2mp \equiv 1 \pmod 3$. Starting with $A(1) = 2$, $A(2) = 3$, and $A(220) = 5$, Sierpiński's Conjecture follows by induction on k.

k	m_k	k	m_k	k	m_k	k	m_k	k	m_k	k	m_k	k	m_k	k	m_k
2	1	77	9072	152	10080	227	26880	302	218880	377	165888	452	990720	527	2677248
3	2	78	38640	153	13824	228	323136	303	509184	378	436800	453	237600	528	5634720
4	4	79	9360	154	23760	229	56160	304	860544	379	982080	454	69120	529	411840
5	8	80	81216	155	13440	230	137088	305	46080	380	324000	455	384000	530	2948400
6	12	81	4032	156	54720	231	73920	306	67200	381	307200	456	338688	531	972000
7	32	82	5280	157	47040	232	165600	307	133056	382	496800	457	741888	532	2813184
8	36	83	4800	158	16128	233	184800	308	82944	383	528768	458	86400	533	3975552
9	40	84	4608	159	48960	234	267840	309	114048	384	1114560	459	1575936	534	368640
10	24	85	16896	160	139392	235	99840	310	48384	385	1609920	460	248832	535	529920
11	48	86	3456	161	44352	236	174240	311	43200	386	485760	461	151200	536	2036736
12	160	87	3840	162	25344	237	104832	312	1111968	387	1420800	462	1176000	537	751680
13	396	88	10800	163	68544	238	23040	313	1282176	388	864864	463	100800	538	233280
14	2268	89	9504	164	55440	239	292320	314	239616	389	959616	464	601344	539	463680
15	704	90	18000	165	21120	240	93600	315	1135680	390	1085760	465	216000	540	2042880
16	312	91	23520	166	46656	241	93312	316	274560	391	264960	466	331776	541	3018240
17	72	92	39936	167	15840	242	900000	317	417600	392	470016	467	337920	542	2311680
18	336	93	5040	168	266400	243	31680	318	441600	393	400896	468	95040	543	1368000
19	216	94	26208	169	92736	244	20160	319	131040	394	211200	469	373248	544	3120768
20	936	95	27360	170	130560	245	62208	320	168480	395	404352	470	559872	545	1723680
21	144	96	6480	171	88128	246	37440	321	153600	396	77760	471	228096	546	1624320
22	624	97	9216	172	123552	247	17280	322	168000	397	112320	472	419328	547	262080
23	1056	98	2880	173	20736	248	119808	323	574080	398	1148160	473	762048	548	696960
24	1760	99	26496	174	14400	249	364800	324	430560	399	51840	474	342720	549	1889280
25	360	100	34272	175	12960	250	79200	325	202752	400	152064	475	918720	550	734400
26	2560	101	23328	176	8640	251	676800	326	707616	401	538560	476	917280	551	842400
27	384	102	28080	177	270336	252	378000	327	611520	402	252000	477	336000	552	874368
28	288	103	7680	178	11520	253	898128	328	317952	403	269568	478	547200	553	971520
29	1320	104	29568	179	61440	254	105600	329	624960	404	763776	479	548352	554	675840
30	3696	105	91872	180	83520	255	257040	330	116640	405	405504	480	129600	555	4306176
31	240	106	59040	181	114240	256	97920	331	34560	406	96768	481	701568	556	1203840
32	768	107	53280	182	54432	257	176256	332	912000	407	1504800	482	115200	557	668160
33	9000	108	82560	183	85536	258	264384	333	72576	408	476928	483	1980000	558	103680
34	432	109	12480	184	172224	259	244800	334	480000	409	944640	484	1291680	559	2611200
35	7128	110	26400	185	136800	260	235872	335	110880	410	743040	485	1199520	560	820800
36	4200	111	83160	186	44928	261	577920	336	1259712	411	144000	486	556416	561	663552
37	480	112	10560	187	27648	262	99360	337	1350720	412	528000	487	359424	562	282240
38	576	113	29376	188	182400	263	64800	338	250560	413	1155840	488	1378080	563	3538944
39	1296	114	6720	189	139104	264	136080	339	124416	414	4093440	489	2088000	564	861120
40	1200	115	31200	190	48000	265	213120	340	828000	415	134400	490	399168	565	221760
41	15936	116	7200	191	102816	266	459360	341	408240	416	258048	491	145152	566	768000
42	3312	117	8064	192	33600	267	381024	342	74880	417	925344	492	2841600	567	2790720
43	3072	118	54000	193	288288	268	89856	343	1205280	418	211680	493	1622880	568	953856
44	3240	119	6912	194	286848	269	101376	344	192000	419	489600	494	1249920	569	7138368
45	864	120	43680	195	59904	270	347760	345	370944	420	1879200	495	2152800	570	655200
46	3120	121	32400	196	118800	271	124800	346	57600	421	1756800	496	2455488	571	3395520
47	7344	122	153120	197	100224	272	110592	347	1181952	422	90720	497	499200	572	3215520
48	3888	123	225280	198	176400	273	171360	348	1932000	423	376320	498	834624	573	2605824
49	720	124	9600	199	73440	274	510720	349	1782000	424	1461600	499	1254528	574	1057536
50	1680	125	15552	200	174960	275	235200	350	734976	425	349920	500	2363904	575	1884960
51	4992	126	4320	201	494592	276	25920	351	473088	426	158400	501	583200	576	3210240
52	17640	127	91200	202	38400	277	96000	352	467712	427	513216	502	1029600	577	1159200
53	2016	128	68640	203	133632	278	464640	353	556800	428	715392	503	2519424	578	4449600
54	1152	129	5760	204	38016	279	200448	354	2153088	429	876960	504	852480	579	272160
55	6000	130	49680	205	50688	280	50400	355	195840	430	618240	505	1071360	580	913920
56	12288	131	159744	206	71280	281	30240	356	249600	431	772800	506	3961440	581	393120
57	4752	132	16800	207	36288	282	157248	357	274176	432	198720	507	293760	582	698880
58	2688	133	19008	208	540672	283	277200	358	767232	433	369600	508	1065600	583	2442240
59	3024	134	24000	209	112896	284	228480	359	40320	434	584640	509	516096	584	6914880
60	13680	135	24960	210	261120	285	357696	360	733824	435	708480	510	616896	585	695520
61	9984	136	122400	211	24192	286	199584	361	576576	436	522720	511	639360	586	497664
62	1728	137	22464	212	57024	287	350784	362	280800	437	884736	512	4014720	587	808704
63	1920	138	87120	213	32256	288	134784	363	63360	438	1421280	513	266112	588	2146176
64	2400	139	228960	214	75600	289	47520	364	1351296	439	505440	514	2386944	589	2634240
65	7560	140	78336	215	42240	290	238464	365	141120	440	836352	515	126720	590	4250400
66	2304	141	25200	216	619920	291	375840	366	399360	441	60480	516	2469600	591	2336256
67	22848	142	84240	217	236160	292	236544	367	168960	442	1836000	517	2819520	592	1516320
68	8400	143	120000	218	70560	293	317520	368	194400	443	866880	518	354816	593	268800
69	29160	144	183456	219	291600	294	166320	369	1067040	444	1537920	519	1599360	594	656640
70	5376	145	410112	220	278400	295	312000	370	348480	445	1219680	520	295680	595	1032192
71	3360	146	88320	221	261360	296	108864	371	147840	446	349440	521	1271808	596	4743360
72	1440	147	12096	222	164736	297	511488	372	641520	447	184320	522	304128	597	4101120
73	13248	148	18720	223	66240	298	132480	373	929280	448	492480	523	3941280	598	2410560
74	11040	149	29952	224	447120	299	354240	374	1632000	449	954720	524	422400	599	9922560
75	27720	150	15120	225	55296	300	84480	375	107520	450	1435200	525	80640	600	427680
76	21840	151	179200	226	420000	301	532800	376	352512	451	215040	526	508032		

TABLE 2. Smallest solution to $A(m) = k$

Table 2 of [34] lists the smallest m, denoted m_k, for which $A(m) = k$ for $2 \leqslant k \leqslant 100$. We extend the computation to $k \leqslant 600$, listing m_k for $k \leqslant 600$ in Table 2.

7.3 Carmichael's Conjecture

The basis for computations of lower bounds for a counterexample to Carmichael's Conjecture is the following Lemma of Carmichael [5], as refined by Klee [24]. For short, let $s(n) = \prod_{p|n} p$ denote the square-free kernel of n.

Lemma 7.2. *Suppose $\phi(x) = m$ and $A(m) = 1$. If $d|x$, $e|\frac{x/d}{s(x/d)}$ and $P = 1 + e\phi(d)$ is prime, then $P^2|x$.*

From Lemma 7.2 it is easy to deduce $2^2 3^2 7^2 43^2 | x$. Here, following Carmichael, we break into two cases: (I) $3^2 \parallel x$ and (II) $3^3|x$. In case (I) it is easy to show that $13^2|x$. From this point onward Lemma 7.2 is used to generate a virtually unlimited set of primes P for which $P^2|x$. In case (I) we search for P using $d = 1, e = 6k$ or $d = 9, e = 2k$, where k is a product of distinct primes (other than 2 or 3) whose squares we already know divide x. That is, if $6k+1$ or $12k+1$ is prime, its square divides x. In case (II) we try $d = 9, e = 2k$ and $d = 27, e = k$, i.e. we test whether or not $6k+1$ and $18k+1$ are primes.

As in [34], certifying that a number P is prime is accomplished with the following lemma of Lucas, Lehmer, Brillhart and Selfridge.

Lemma 7.3. *Suppose, for each prime q dividing $n-1$, there is a number a_q satisfying $a_q^{n-1} \equiv 1$ and $a_q^{(n-1)/q} \not\equiv 1 \pmod{n}$. Then n is prime.*

The advantage of using Lemma 7.3 in our situation is that for a given P we are testing, we already know the prime factors of $P - 1$ (i.e. 2,3 and the prime factors of k).

Our overall search strategy differs from [34]. In each case, we first find a set of 32 "small" primes P (from here on, P will represent a prime generated from Lemma 7.2 for which $P^2|x$, other than 2 or 3). Applying Lemma 7.2, taking k to be all possible products of 1,2,3 or 4 of these 32 primes yields a set S of 1000 primes P, which we order $p_1 < \cdots < p_{1000}$. This set will be our base set. In particular, $p_{1000} = 796486033533776413$ in case (I) and $p_{1000} = 78399428950769743507519$ in case (II). The calculations are then divided into "runs". For run #0, we take for k all possible combinations of 1,2 or 3 of the primes in S. For $j \geqslant 1$, run #j tests every k which is the product of p_j and three larger primes in S. Each candidate P is first tested for divisibility by small primes and must pass the strong pseudoprime test with bases 2,3,5,7,11 and 13 before attempting to certify that it is prime. There are two advantages to this approach. First, the candidates P are relatively small (the numbers tested in case (I) had an average of 40 digits and the numbers tested in case (II) had an average of 52 digits). Second, $P - 1$ has at most 6 prime factors, simplifying the certification process. To achieve $\prod P^2 > 10^{10^{10}}$, 13 runs were required in case (I) and 14 runs were required in case (II). Together these runs give Theorem 6. A total of 126,520,174 primes were found in case (I), and 104,942,148 primes were found in case (II). The computer program was written in GNU C, utilizing Arjen Lenstra's Large Integer Package, and run on a network of 200MHz Pentium PCs running LINUX O/S in December 1996 (4,765 CPU hours total).

In 1991, Pomerance (see [30] and [25]) showed that

$$\liminf_{x\to\infty} \frac{V_1(x)}{V(x)} \leqslant \frac{1}{2}. \tag{7.1}$$

A modification of his argument, combined with the above computations, yields the much stronger bound in Theorem 7. Recall that $V(x;k)$ counts the totients $\leqslant x$, all of whose preimages are divisible by k.

Lemma 7.4. *We have $V(x;a^2) \leqslant V(x/a)$.*

Proof. The lemma is trivial when $a = 1$ so assume $a \geqslant 2$. Let n be a totient with $x/a < n \leqslant x$. First we show that for some integer $s \geqslant 0$, $a^{-s}n$ is a totient with an pre-image not divisible by a^2. Suppose

$\phi(m) = n$. If $a^2 \nmid m$, take $s = 0$. Otherwise we can write $m = a^t r$, where $t \geqslant 2$ and $a \nmid r$. Clearly $\phi(ar) = a^{1-t}n$, so we take $s = t - 1$. Next, if n_1 and n_2 are two distinct totients in $(x/a, x]$, then $a^{-s_1}n_1 \neq a^{-s_2}n_2$ (since n_1/n_2 cannot be a power of a), so the mapping from totients in $(x/a, x]$ to totients $\leqslant x$ with a pre-image not divisible by a^2 is one-to-one. Thus $V(x) - V(x; a^2) \geqslant V(x) - V(x/a)$. □

The above computations show that if $\phi(x) = n$ and $A(n) = 1$, then x is divisible by either a^2 or b^2, where a and b are numbers greater than $10^{5,001,850,000}$. Suppose $a \leqslant b$. By Lemma 7.4, we have

$$V_1(x) \leqslant V(x/a) + V(x/b) \leqslant 2V(x/a). \tag{7.2}$$

Lemma 7.5. *Suppose $a > 1$, $b > 0$ and $V_1(x) \leqslant bV(x/a)$ for all x. Then*

$$\liminf_{x\to\infty} \frac{V_1(x)}{V(x)} \leqslant \frac{b}{a}.$$

Proof. Suppose $c = \liminf_{x\to\infty} \frac{V_1(x)}{V(x)} > 0$. For every $\varepsilon > 0$ there is a number x_0 such that $x \geqslant x_0$ implies $V_1(x)/V(x) \geqslant c - \varepsilon$. For large x, set $n = [\log(x/x_0)/\log a]$. Then

$$\begin{aligned} V(x) &= \frac{V(x)}{V(x/a)} \frac{V(x/a)}{V(x/a^2)} \cdots \frac{V(x/a^{n-1})}{V(x/a^n)} V(x/a^n) \\ &\leqslant b^n \frac{V(x)}{V_1(x)} \frac{V(x/a)}{V_1(x/a)} \cdots \frac{V(x/a^{n-1})}{V_1(x/a^{n-1})} V(ax_0) \\ &\leqslant b^n (c-\varepsilon)^{-n}(ax_0) = O(x^{-\log((c-\varepsilon)/b)/\log a}). \end{aligned}$$

This contradicts the trivial bound $V(x) \gg x/\log x$ if $c > \frac{b}{a} + \varepsilon$. Since ε is arbitrary, the lemma follows. □

Theorem 7 follows immediately. Further improvements in the lower bound for a counterexample to Carmichael's Conjecture will produce corresponding upper bounds on $\liminf_{x\to\infty} V_1(x)/V(x)$. Explicit bounds for the $O(1)$ term appearing in Theorem 1 (which would involve considerable work to obtain) combined with (7.2) should give a strong upper bound for $\limsup_{x\to\infty} V_1(x)/V(x)$.

Next, suppose d is a totient, all of whose pre-images m_i are divisible by k. The lower bound argument given in Section 5 shows that for at least half of the numbers $b \in \mathscr{B}$, the totient $\phi(b)d$ has only the pre-images bm_i. In particular, all of the pre-images of such totients are divisible by k and Theorem 8 follows.

It is natural to ask for which k do there exist totients, all of whose pre-images are divisible by k. A short search reveals examples for each $k \leqslant 11$ except $k = 6$ and $k = 10$. For $k \in \{2, 4, 8\}$, take $d = 2^{18} \cdot 257$, for $k \in \{3, 9\}$, take $d = 54 = 2 \cdot 3^3$, for $k = 5$ take $d = 12500 = 4 \cdot 5^5$, for $k = 7$, take $d = 294 = 6 \cdot 7^2$ and for $k = 11$, take $d = 110$. It appears that there might not be any totient, all of whose pre-images are divisible by 6, but I cannot prove this. Any totient with a unique pre-image must have that pre-image divisible by 6, so the non-existence of such numbers implies Carmichael's Conjecture.

I believe that obtaining the asymptotic formula for $V(x)$ will require simultaneously determining the asymptotics of $V_k(x)/V(x)$ (more will be said in section 8) and $V(x;k)/V(x)$ for each k. It may even be necessary to classify totients more finely. For instance, taking $d = 4, k = 4$ in the proof of Theorem 2 (section 5), the totients m constructed have $\phi^{-1}(m) = \{5n, 8n, 10n, 12n\}$ for some n. On the other hand, taking $d = 6, k = 4$ produces a different set of totients m, namely those with $\phi^{-1}(m) = \{7n, 9n, 14n, 18n\}$ for some n. Likewise, for any given d with $A(d) = k$, the construction of totients in Section 5 may miss whole classes of totients with multiplicity k. There is much further work to be done in this area.

8 Generalization to other multiplicative functions

The proofs of our theorems easily generalize to a wide class of multiplicative arithmetic functions with similar behavior on primes, such as $\sigma(n)$, the sum of divisors function. If $f : \mathbb{N} \to \mathbb{N}$ is a multiplicative arithmetic function, we analogously define

$$\begin{gathered}\mathscr{V}_f = \{f(n) : n \in \mathbb{N}\}, \quad V_f(x) = |\mathscr{V}_f \cap [1, x]|, \\ f^{-1}(m) = \{n : f(n) = m\},\ A_f(m) = |f^{-1}(m)|,\ V_{f,k}(x) = |\{m \leqslant x : A_f(m) = k\}|.\end{gathered} \tag{8.1}$$

We now indicate the modifications to the previous argument needed to prove Theorem 14. By itself, condition (1.11) is enough to prove the lower bound for $V_f(x)$. Condition (1.12) is used only for the upper bound argument and the lower bound for $V_{f,k}(x)$.

The function $f(n) = n$, which takes all positive integer values, is an example of why zero must be excluded from the set in (1.11). Condition (1.12) insures that the values of $f(p^k)$ for $k \geqslant 2$ are not too small too often, and thus have little influence on the size of $V_f(x)$. It essentially forces $f(h)$ to be a bit larger than $h^{1/2}$ on average. It's probable that (1.12) can be relaxed, but not too much. For example, the multiplicative function defined by $f(p) = p - 1$ for prime p, and $f(p^k) = p^{k-1}$ for $k \geqslant 2$ clearly takes all integer values, while

$$\sum_{h \geqslant 4,\ \text{square-full}} \frac{1}{f(h)(\log_2 h)^2} \ll 1.$$

Condition (1.12) also insures that $A(m)$ is finite for each f-value m. For example, a function satisfying $f(p^k) = 1$ for infinitely many prime powers p^k has the property that $A(m) = \infty$ for every f-value m.

In general, implied constants will depend on the function $f(n)$. One change that must be made throughout is to replace every occurrence of "$p - 1$" (when referring to $\phi(p)$) with "$f(p)$", for instance in the definition of S-normal primes in Section 2. Since the possible values of $f(p) - p$ is a finite set, Lemma 2.6 follows easily with the new definitions. The most substantial change to be made in Section 2, however, is to Lemma 2.7, since we no longer have the bound $n/f(n) \ll \log_2 n$ at our disposal.

Lemma 2.7*. *The number of $m \in \mathscr{V}_f(x)$ for which either $d^2|m$ or $d^2|n$ for some $n \in f^{-1}(m)$ and $d > Y$ is $O(x(\log_2 x)^K/Y^{2\delta})$, where $K = \max_p(p - f(p))$.*

Proof. The number of m with $d^2|m$ for some $d > Y$ is $O(x/Y)$. Now suppose $d^2|n$ for some $d > Y$, and let $h = h(n)$ be the square-full part of n (the largest squarefull divisor of n). In particular, $h(n) > Y^2$. From the fact that $f(p) \geqslant p - K$ for all primes p, we have

$$f(n) = f(h)f(n/h) \gg \frac{f(h)n}{h}(\log_2(n/h))^{-K}.$$

Thus, if $f(n) \leqslant x$, then

$$\frac{n}{h}\left(\log_2 \frac{n}{h}\right) \ll \frac{x}{f(h)}.$$

Therefore, the number of possible n with a given h is crudely $\ll x(\log_2 x)^K/f(h)$. By (1.12), the total number of n is at most

$$\ll x(\log_2 x)^K \sum_{h \geqslant Y^2} \frac{1}{f(h)} \ll \frac{x(\log_2 x)^K}{Y^{2\delta}} \sum_h \frac{h^\delta}{f(h)} \ll \frac{x(\log_2 x)^K}{Y^{2\delta}}. \qquad \square$$

Applying Lemma 2.7* in the proof of Lemma 2.8 with $Y = S^{1/2}$ yields the same bound as claimed, since $S > \exp\{(\log_2 x)^{36}\}$.

In Section 3, the only potential issue is with Lemma 3.1, but the analog of t_m is $\ll \exp\{-\delta e^{m-1}\}$.

The only modification needed in Section 4 comes from the use of $\phi(ab) \geqslant \phi(a)\phi(b)$ in the argument leading to (4.10). If $q_L \nmid w$, the existing argument is fine. If $q_L|w$, let $j = \max\{i \leqslant L : q_i < q_{i-1}\}$. Since $q_{L-2} > q_L$, $j \in \{L-1, L\}$. Write $f(q_1 \cdots q_L w) = f(q_1 \cdots q_{j-1})f(w')$, where $w' = q_j \cdots q_L w$ and $(x_1, \ldots, x_j) \in \mathscr{R}_j(\mathscr{S}_j((\xi_1, \ldots, \xi_{j-1}))$. Put $v = f(w')$, use the analog of (4.6) to bound $\sum 1/v$, and otherwise follow the argument leading to (4.10).

In Section 5, there are several changes. For Lemma 5.1, the equation (5.1) may have trivial solutions coming from pairs p, p' with $f(p) = f(p')$. We say a prime p is "bad" if $f(p) = f(p')$ for some prime $p' \neq p$ and say p is "good" otherwise. By (1.11) and Lemma 2.5, the number of bad primes $\leqslant y$ is $O(y/\log^2 y)$, so $\sum_{p\, bad} 1/p$ converges. In Lemma 5.1, add the hypothesis that the p_i and q_i are all "good". Possible small values of $f(p^k)$ for some p^k with $k \geqslant 2$ are another complication. For each prime p, define

$$Q(p) := \min_{k \geqslant 2} \frac{f(p^k)}{f(p)}. \tag{8.2}$$

Introduce another parameter d (which will be the same d as in Theorem 2) and suppose $L \leqslant L_0 - M$ where M is a sufficiently large constant depending on P_0 and d. If follows from (1.12) and (8.2) that

$$\sum_{Q(p) \leqslant d} \frac{1}{p} = O(d).$$

In the definition of $\mathscr{B}$, add the hypothesis that all primes p_i are "good" and replace (5.16) by $Q(p_i) \geqslant \max(d + K + 1, 17)$ for every i. Of course, (5.13) is changed to $f(n) \leqslant x/d$. Fortunately, the numbers in $\mathscr{B}$ are square-free by definition. Consider the analog of (5.18). Since $Q(p_i) > d + K$ for each p_i, if $n | n_1$ and one of the primes q_i ($0 \leqslant i \leqslant L$) occurs to a power greater than 1, then $\phi(n_1) > d\phi(n)$. Therefore, the $L+1$ largest prime factors of n_1 occur to the first power only, which forces $n_1 = nm_i$ for some i (the trivial solutions). For nontrivial solutions, we have at least one index i for which $p_i \neq q_i$, and hence $f(p_i) \neq f(q_i)$ (since each p_i is "good"). Other changes are more obvious.: In (5.5), the phrase "$rt + 1$ and $st + 1$ are unequal primes" is replace by "$rt + a$ and $st + a'$ are unequal primes for some pair of numbers (a, a') with $a, a' \in \mathscr{P}$." Here $\mathscr{P}$ denotes the set of possible values of $f(p) - p$. As $\mathscr{P}$ is finite, this poses no problem in the argument. Similar changes are made in several places in the argument leading to (5.7).

Only small, obvious changes are needed for Theorem 16. The rest of Section 6 needs very little attention, as the bounds ultimately rely on Lemma 3.1 and the volume computations (which are independent of f).

It is not possible to prove analogs of Theorems 5–9 for general f satisfying the hypotheses of Theorem 14. One reason is that there might not be any "Carmichael Conjecture" for f, e.g. $A_\sigma(3) = 1$, where σ is the sum of divisors function. Furthermore, the proof of Theorem 9 depends on the identity $\phi(p^2) = p\phi(p)$ for primes p. If, for some $a \neq 0$, $f(p) = p + a$ for all primes p, then the argument of [15] shows that if the multiplicity k is possible and r is a positive integer, then the multiplicity rk is possible. For functions such as $\sigma(n)$, for which the multiplicity 1 is possible, this completely solves the problem of the possible multiplicities. For other functions, it shows at least that a positive proportion of multiplicities are possible. If multiplicity 1 is not possible, and $f(p^2) = pf(p)$, the argument in [16] shows that all multiplicities beyond some point are possible.

We can, however, obtain information about the possible multiplicities for more general f by an induction argument utilizing the next lemma. Denote by $a_1, \dots, a_K$ the possible values of $f(p) - p$ for prime p.

Lemma 7.1*. *Suppose $A_f(m) = k$. Let p, q, s be primes and $r \geqslant 2$ an integer so that*

(1) *(i) s and q are "good" primes,*
(2) *(ii) $mf(s) = f(q)$,*
(3) *(iii) $f(s) = rp$,*
(4) *(iv) $p \nmid f(\pi^b)$ for every prime π, integer $b \geqslant 2$ with $f(\pi^b) \leqslant mf(s)$,*
(5) *(v) $dp - a_i$ is composite for $1 \leqslant i \leqslant K$ and $d | rm$ except $d = r$ and $d = rm$.*

Then $A_f(mrp) = k + A_f(1)$.

Proof. Let $f^{-1}(m) = \{x_1, \dots, x_k\}$ and suppose $f(x) = mrp$. By condition (iv), $p | f(\pi)$ for some prime π which divides x to the first power. Therefore, $f(\pi) = dp$ for some divisor d of mr. Condition (v) implies that the only possibilities for d are $d = r$ or $d = rm$. If $d = r$, then $f(\pi) = rp = f(p)$ which forces

$\pi = s$ by condition (i). By conditions (ii) and (iii), we have $f(x/s) = m$, which gives solutions $x = sx_i$ $(1 \leqslant i \leqslant k)$. Similarly, if $d = rm$, then $\pi = q$ and $f(x/q) = 1$, which has $A_f(1)$ solutions. □

By the Chinese Remainder Theorem, there is an arithmetic progression $\mathscr{A}$ so that condition (v) is satisfied for each number $p \in \mathscr{A}$, while still allowing each $rp + a_i$ and $rmp + a_i$ to be prime. To eliminate primes failing condition (iv), we need the asymptotic form of the Prime k-tuples Conjecture due to Hardy and Littlewood [21] (actually only the case where $a_i = 1$ for each i is considered in [21]; the conjectured asymptotic for k arbitrary polynomials can be found in [3]).

Conjecture 2 (Prime k-tuples Conjecture (asymptotic version)**.** *Suppose $a_1, \ldots, a_k$ are positive integers and $b_1, \ldots, b_k$ are integers so that no prime divides $(a_1 n + b_1) \cdots (a_k n + b_k)$ for every integer n. Then for some constant $C(\mathbf{a}, \mathbf{b})$, the number of $n \leqslant x$ for which $a_1 n + b_1, \ldots, a_k n + b_k$ are simultaneously prime is*

$$\sim C(\mathbf{a}, \mathbf{b}) \frac{x}{\log^k x} \qquad (x \geqslant x_0(\mathbf{a}, \mathbf{b})).$$

Using (1.12), we readily obtain $|\{\pi^b : f(\pi^b) \leqslant y, b \geqslant 2\}| \ll y^{1-\delta}$. If s is taken large enough, the number of possible $p \leqslant x$ satisfying condition (iv) (assuming r and m are fixed and noting condition (iii)) is $o(x/\log^3 x)$. The procedure for determining the set of possible multiplicities with this lemma will depend on the behavior of the particular function. Complications can arise, for instance, if m is even and all of the a_i are even (which makes condition (ii) impossible) or if the number of “bad” primes is $\gg x/\log^3 x$.

References

[1] R. C. Baker and G. Harman, *Shifted primes without large prime factors*, Acta Arith. **83** (1998), 331–361.

[2] R. C. Baker, G. Harman and J. Pintz, *The difference between consecutive primes. II.*, Proc. London Math. Soc. (3) **83** (2001), no. 3, 532–562.

[3] P. T. Bateman and R. A. Horn , *A heuristic asymptotic formula concerning the distribution of prime numbers* , Math. Comp. **16** (1962), 363–367.

[4] R. D. Carmichael , *On Euler's ϕ-function* , Bull. Amer. Math. Soc. **13** (1907) , 241–243.

[5] ———, *Note on Euler's ϕ-function* , Bull. Amer. Math. Soc. **28** (1922) , 109–110.

[6] E. Cohen , *Arithmetical functions associated with the unitary divisors of an integer* , Math. Z. **74** (1960) , 66–80.

[7] L. E. Dickson , *A new extension of Dirichlet's theorem on prime numbers* , Messenger of Math. **33** (1904) , 155–161.

[8] P. Erdős , *On the normal number of prime factors of $p-1$ and some related problems concerning Euler's ϕ-function* , Quart. J. Math. Oxford **6** (1935), 205-213.

[9] ———, *Some remarks on Euler's ϕ-function and some related problems* , Bull. Amer. Math. Soc. **51** (1945), 540–544.

[10] ———, *Some remarks on Euler's ϕ-function* , Acta Arith. **4** (1958), 10–19.

[11] P. Erdős and R.R.Hall , *On the values of Euler's ϕ-function* , Acta Arith. **22** (1973), 201-206.

[12] ———, *Distinct values of Euler's ϕ-function* , Mathematika **23** (1976), 1–3.

[13] P. Erdős and C. Pomerance, *On the normal number of prime factors of $\phi(n)$* , Rocky Mountain J. of Math. **15** (1985), 343–352.

[14] K. Ford, *The distribution of totients*, Ramanujan J. (Paul Erdős memorial issue) **2** (1998), 67–151.

[15] K. Ford and S. Konyagin, *On two conjectures of Sierpiński concerning the arithmetic functions σ and ϕ*, Number Theory in Progress (Zakopane, Poland, 1997), vol. II, de Gruyter (1999), 795-803.

[16] K. Ford , *The number of solutions of $\phi(x) = m$* , Annals of Math. **150** (1999), 283–311.

[17] K. Ford and K.-W. Lau, *Asymptotics of a recurrence sequence: Solution of Problem 10682*, Amer. Math. Monthly **107** (2009), 374–375.

[18] J. Friedlander, *Shifted primes without large prime factors*, in Number theory and applications (Banff, AB, 1988) , Kluwer Acad. Publ., Dorbrecht (1989), 393–401.

[19] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London , 1974.

[20] R. R. Hall and G. Tenenbaum, *Divisors*, Cambridge University Press, 1988.

[21] G. H. Hardy and J. E. Littlewood, *Some problems of 'Partitio Numerorum': III. On the representation of a number as a sum of primes*, Acta Math. **44** (1923), 1–70.

[22] G. H. Hardy and S. Ramanujan , *The normal number of prime factors of a number n* , Quart. J. Math. **48** (1917), 76–92.

[23] A. Hildebrand and G. Tenenbaum , *Integers without large prime factors* , J. Théor. Nombres Bordeaux **5** (1993), 411–484.

[24] V. Klee , *On a conjecture of Carmichael* , Bull. Amer. Math. Soc. **53** (1947), 1183–1186.

[25] Mattics, L. E. , *A half step towards Carmichael's Conjecture, Solution to Problem 6671* , Amer. Math. Monthly **100** (1993), 694–695.

[26] H. Maier and C. Pomerance , *On the number of distinct values of Euler's ϕ-function* , Acta Arith. **49** (1988), 263–275.

[27] P. Masai and A. Valette , *A lower bound for a counterexample to Carmichael's Conjecture*, Bollettino U.M.I. (6) **1** (1982), 313–316.

[28] S. Pillai , *On some functions connected with $\phi(n)$* , Bull. Amer. Math. Soc. **35** (1929), 832–836.

[29] C. Pomerance , *On the distribution of the values of Euler's function* , Acta Arith. **47** (1986), 63–70.

[30] ______, *Problem 6671*, Amer. Math. Monthly **98** (1991), 862.

[31] A. Schinzel , *Sur l'equation $\phi(x) = m$* , Elem. Math. **11** 1956, 75–78.

[32] ______, *Remarks of the paper "Sur certaines hypothèses concernant les nombres premiers"* , Acta Arith. **7** (1961/62), 1–8.

[33] A. Schinzel and W. Sierpiński , *Sur certaines hypothèses concernant les nombres premiers* , Acta Arith. **4** (1958), 185–208.

[34] A. Schlafly and S. Wagon , *Carmichael's conjecture on the Euler function is valid below $10^{10,000,000}$* , Math. Comp. **63** (1994), 415–419.